(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/23808 A2

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/US01/28628

(22) International Filing Date:
14 September 2001 (14.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/662,058 15 September 2000 (15.09.2000) US

(71) Applicant: CYMTEC SYSTEMS, INC. [US/US]; 8000 Maryland Avenue, Suite 700, Clayton, MO 63105 (US).

(72) Inventor: MESTER, Michael, L.; 816 C Westbrooke Village Drive, St. Louis, MO 63021 (US).

(74) Agents: KANG, Grant, D. et al.; Thompson Coburn LLP, One Firstar Plaza, St. Louis, MO 60101 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/23808 A2

(54) Title: NETWORK MANAGEMENT SYSTEM

(57) Abstract: The invention is a network management system that is placed in communication with an existing network. The network management system interposes an intermediate advanced intelligence device between the network management system and the client network. This insertion functions to provide additional security, communication ability and decision-making ability to the management of network systems. The network management system combines trending performance management with intrusion detection to develop an event correlation from multiple data sources. Specifically, data is gathered from multiple sources, a correlation between events and performance data as it relates to security and system optimization, is created, and information is provided to a monitor at the network management system, with additional information provided to a user at the existing network location.

NETWORK MANAGEMENT SYSTEM

Cross-Reference to Related Applications

None.

Statement Regarding Federally Sponsored Research or Development.

Not Applicable.

Background of the Invention

1. Field of the Invention

This invention relates to computer network management systems and, more particularly, to a computer network management system that provides understandable information to an end user. More specifically, the invention collects information from a client computer network and translates data into an understandable format for display to the end user. In doing so, the invention provides a way to provide secure network management services to third parties.

2. Related Art

Currently, computer networks provide information to end users such as network administrators in the form of statistical data. For example, a network administrator may obtain reports that provide information such as number of transmitted bytes of information transmitted across an interface, the number of packets transmitted and received over a particular link, the number of ports in use. Interface in errors, interface in/out octets, inbound/outbound unicast

packets, inbound/outbound non-unicast packets. This information is simply illustrative of the fact that a network administrator has a specific software solution package that provides specific statistical information about specific activities occurring on or within a computer network. A standard in the industry for collecting such information is SNMP (Simple Network Management Protocol). HP Openview and Computer Associates Unicenter TNG are two commercially available software packages that utilize SNMP to provide this statistical information.

Similarly, other specific software packages exist to monitor and address other issues. For example, security software packages monitor and provide statistical information on security-related subjects such as, but not limited to, intrusion detection, system vulnerability, virus detection and policy violation. An example of such a software package commonly available in the industry is sold under the trade name NetRanger Intrusion Detection System. There are numerous other software packages for achieving the similar goal of security monitoring which are sold under the trade names Real Secure, Nessus, Tcpdump, Ethereal, Dsniff, SATAN, scanlogd, snort, SARA, and logcheck.

An example of yet another specific software package is performance management software. Examples of products currently available and sold under various trade names include Visual Networks Visual Uptime, Iplog, and IPTraf.

Another example of specific software packages used in Network Management, and commonly available commercially are Openview, IBM Tivoli and Unicenter TNG.

Published reports have revealed that implementation of these software packages has been largely unsuccessful. Indeed, the GartnerGroup found that one-third of companies that had bought their own network management systems had not implemented them within three years of

the purchase. See, Adams, Steve, "Performing for the NGN", Telecommunications International Edition, August 1999.

In addition, it should be recognized that these software packages are so specialized that it requires significant and specialized training to educate a network administrator in the operation and use of data of each package. For example, information relating to in/out octets must be carefully interpreted by a network administrator so that the operation of the specific individual network and specific system configuration must be considered. This octet information may be widely divergent on different systems but lead to the same conclusion, given the differences of specific networks and configurations. More specifically, a network administrator may receive a report showing "5,000 octets". The network administrator must then interpret this data in view of: time since last system reset, time since last counter cycle and related interface speed (a system running at a gigabit rate versus a system running at a megabit rate). This single example of the interpretation of data is illustrative of the challenge facing a network administrator in reviewing the reams of data pumped out by each of these specific network software packages. Accordingly, the job of a network administrator in interpreting all of these extremely specialized statistics emanating from these increasingly-specialized software packages is impossible. No one person can any longer develop or maintain expertise in each of the software packages available or in use.

Therefore, in recognition of these difficulties, a single network administrator position has been often split into multiple network administrator positions. Each of the new network administrators develops deep expertise in specific software packages. When a problem in the network occurs, the multiple network administrators must confer with each other to determine

the origin of the problem and jointly agree on a proposed course of action for solving the problem. Due to the transactional speed of events occurring over the network, when a problem occurs under this new model of multiple network administrators, any problem must necessarily be addressed after the fact, with nothing remotely approaching a real time solution.

The specialization of network administrators has also created a new corps of intrusion detection network administrators. These network administrators work throughout various companies on different networks. However, these administrators confer with each other regularly regarding new or unusual network activity. Together, these administrators must share enough information in order to determine whether their networks are under attack. However, this sharing of information violates most security policies by disseminating detailed information regarding network configuration to third parties, thereby further increasing the risk of future intrusion.

This multiple network administrator model leads then to additional problem solving conferences that quickly overload administrator resources. A catch-22 situation arises. A single network administrator cannot possibly keep up with the expertise required in understanding the data from all of the varied specialty software packages. Therefore, a multiple administrator model for depth of expertise is required. A multiple administrator model cannot solve problems as quickly as a single network administrator which leads to a delay in problem-solving that can have catastrophic results. Therefore, the decision-making speed of a single administrator model is required.

Thus, the major shortcoming of the current state of the art is the lack of depth in functionality. While the ability to provide a simple up/down management service solution is

common, the linking of trending performance management with intrusion detection is non-existent. In other words, the ability to monitor network activity from the perspective of "event correlation" where cause and effect relationships are generated as problems occur is a tool that allows problems to not only be fixed when the occur, but more importantly to be prevented in the future by using the collected information productively.

Currently, there is a need to provide the depth of expertise existing in a multiple network administrator model, to interpret specialized data flows, combined with the decision-making speed of a single network administrator model, to identify and solve network problems in near real-time.

Summary of the Invention

It is in view of the above problems that the present invention was developed. The invention is a network management system that is placed in communication with an existing network that uses devices (workstation, server, or other client device) employing simple network management protocol (SNMP). From these devices, the network management system selectively extracts data relating to trending performance management, security systems, and intrusion detection.

After extraction, the network management system securely transmits this data from the existing client network through the network management system for processing. The secure transmission of information occurs between a distributed state machine, otherwise known as an advanced intelligence device, and a core site. The addition of an advanced intelligence device to the network is critical to the ability to provide multiple client networks with secure network management services.

During data processing, the network management system creates multiple event correlations between events and performance data. Then, these correlations are provided to a user in the form of a graphical user interface. Specifically, the user obtains information on long term trending, correlated views of critical events happening within a time window relating to a particular device, and other correlations between performance management, security systems, and intrusion detection in order to detect unknown signatures, unknown attack patterns, and other useful information.

Thus, the invention addresses a lack in core functionality of off-the-shelf programs. This correlation provides a higher level of network operation awareness within existing customer networks and Information Technology infrastructure.

The invention of this network management system permits the use of this system to monitor and provide secure service to multiple existing customer networks. This secure service is accomplished by the imposition of an advanced intelligence device between the core site and the customer site. Until now, any third party monitoring and management has been done with be third party network manager making a direct connection with the client network. However, if multiple clients are connected to a single third party network manager, this configuration opens the possibility that one client may obtain records and information from another client via the network. This advanced intelligence device of the present invention is placed between any client and the core. This placement prevents any one client/customer from reaching through the core site to obtain access to a third party client/customer. Each existing customer network will be connected to an advanced intelligent device which is located on the customer premises. Each advanced intelligent device is connected to the customer network, and is in communication with

a remote site. The advanced intelligent device will run performance collection application software to extract data. This data will be transferred to a core network operations center, a remote site, where the data will be correlated with other enterprise management events before finally being processed for viewing. The network management system uses a specialized security transport and data transfer mechanism which is scaleable and adapted towards long-term trending (as opposed to current solutions).

A graphical user interface (GUI), or web interface, will provide the customer with a customized view of the performance of his or her network together with enterprise correlation. The performance management function is granular enough to perform at a specific device level, but is also able to provide information on a global network level.

Further features and advantages of the present invention, as well as the structure and operation of various embodiments of the present invention, are described in detail below with reference to the accompanying drawings.

Brief Description of the Drawings

The accompanying drawings, which are incorporated in and form a part of the specification, illustrate the embodiments of the present invention and together with the description, serve to explain the principles of the invention. In the drawings:

Figure 1 illustrates a block diagram of the management system of the present invention which is in communication with an existing network;

Figure 2 illustrates a detail view of block 2-2 in Figure 1; and

Figure 3 is a block diagram illustrating the dataflow of the agent configuration of the

present invention.

Figure 4 is a block diagram of an intrusion detection system (IDS) ;

Figure 5 is a block diagram of dataflow relating to trend performance collection;

Figure 6 is a block diagram of dataflow relating to a graphical user interface.;

Figure 7 is a block diagram of dataflow relating to a correlating events;

Figure 8 is a view of a Map for display by the client machine of the present invention;

Figure 9 is a view of a Site for display by the client machine of the present invention;

Figure 10 is a view of a Host Detail for display by the client machine of the present invention;

Figure 11 is a view of Router information for display by the client machine of the present invention;

Figure 12 is a view of a tree for display by the client machine of the present invention;

Figure 13 is a view of utilization for display by the client machine of the present invention;

Figure 14 is a view of exceptions for display by the client machines of the present invention;

Figure 15 is a view of intrusion detection for display by the client machines of the present invention;

Figure 16 is a view of correlation for display by the client machines of the present invention;

Figure 17 is a view of reports that are available and can be retrieved for display by the client machines; and

Figure 18 is a view of the display used by the client machine in order to adjust the settings for obtaining information.

Detailed Description of the Preferred Embodiments

Referring to the accompanying drawings in which like reference numbers indicate like elements, Figure 1 illustrates the network management system 20 of the present invention. Network management system 20 comprises advanced intelligence device 32, linked via first encryption/transmission device 34, second encryption/transmission device 36, transaction processor 38, and common media 40 to remote site 42.

Advanced Intelligence Device

Advanced intelligence device 32 comprises first interface card (IC1) 44, first data loader module (DLM) 46, second DLM 48, third DLM 50, configuration module 52, advance artificial intelligence module 54, security module 56, data correlation module 58, transmission control module 60, local database 62, and second interface card (IC2) 64.

First interface card 44 is used to transfer the data requests and receive the data responses from the managed devices. First interface card 44 connects to first common media 40 that client managed devices, shown generally at 66, are attached to. Client managed devices 64 may include data communications equipment 68, servers 70, workstations 72, and security devices 74.

Advanced intelligence device 32 is connected to the client's existing network via first common media 40 (and first interface card 44) on the client's premises. First common media 40 is preferably an ethernet system.

Each of the data loader modules (DLM), first data loader module 46, second data loader module 48, and third data loader module 50, respectively, are derived from remotely located

main database 100. Each DLM 46 – 50 is responsible for loading data from the remote system 96 into the local database 62. Each of the DLMs 46-50, respectively is delivered to local database 62 for faster processing. The function of a DLM, 46-50, respectively, is to instruct the transmission control module 60 on what types of data to retrieve from a managed device 66. Each DLM 46-50 also contains information about the method for obtaining that information. For example, first DLM 46 monitors wide area network link performance. First DLM 46 is also responsible for storing a mathematical formula to make useful data out of the collected statistics. After first DLM 46 modifies data using the stored mathematical formula, the modified data is loaded into local database 62.

Main database 100 is the source for the information in configuration module (CM) 52. Once loaded with information from main database 100, configuration module 52 refreshes local database 62 with periodic updates. Configuration module 52 is designed to configure remote system agents, shown generally at 96, such as operating system agents, shown generally at 98. Operating system agents 98 contain information about a variety of performance characteristics such as percent processor utilization and available memory. Configuration module 52 uses transmission control module 60 to communicate with the appropriate interface card 44, 64. Through the transmission of this data, a remote agent 96 receives configuration updates.

Advance Artificial Intelligence Module (AAIM) 54 reads the data being collected by the DLM's 46-50 and the correlated data provided by DCM 58 from the local database. AAIM 54 is initially retrieved from the remote, main database 100. AAIM 54 provides probability and statistical information about overall system events. These events can contain security, performance, and error conditions. AAIM 54 looks for patterns and over time begins to recognize

network problem sources. AAIM 54 can be automatically updated by the Global Advanced Correlation Module 104. After creating statistical information about above data, AAIM 54 loads its information into the local database 62 for future comparisons. In addition, correlation module 58 polls AAIM 54 for instructions. Then, correlation module 58 proceeds as is set forward in greater detail below.

Before any communication gets passed to transmission control module (TCM) 60 it must first be processed by security module 56. This module 56 provides authentication and authorization information about what information is allowed to be transferred. It also provides secure access to the local database 62.

The local database 62 stores information about agent configuration, client graphical user interface (GUI) information, data loader module 46 - 50, AAIM 54, transaction control module 60, and correlation module 58. Local database 62 also acts as a system proxy agent for remote long-term trending data retrieval from the remote database 100.

TCM 60 is responsible for directing traffic to or receiving traffic from the given interfaces. It also contains detailed knowledge about what methods it is to be using to collect the information. Each method has requirement that must be met prior to sending data to an interface. In this way TCM 60 ensures that the information transmitted is in syntax.

Thus, it can be seen that the advanced intelligent device 32 is connected to the customer network and is in communication with a remote site. The advanced intelligent device 32 runs performance collection application software to extract data.

Once the data is extracted, which is in standard SNMP format, it is communicated via first interface card 44 to transaction control module 60, as seen in Fig. 2. The transaction control

module 60 sends the data to first data loader module 46.

Meanwhile, first data loader module 46 has communicated with local database 62 to store configuration information into memory such as the DLM name, DLM variables, DLM method, the calculation formula, the data loading information, the variance, etc. Using the stored values in memory, first data loader module 46 converts the incoming data from the transaction control module 60 into variables, and applies the formulas resident within the data loader module 46.

First data loader module 46 transmits the results to local database 62 where it is stored, as well as to transaction control module 60. Transaction control module 60 performs a look up to determine the format needed for data transmission, preferably wire data transmission. Once the format is known, transaction control module 60 is placed in communication with the appropriate apis and then sends the data to the appropriate interface.

The data loader modules 46-50 are implemented by using blocks of software code. The code is loaded (or initiated) by local client database 62.

Secure Transmission of Data from Advanced Intelligence Device

Second interface card 64 provides a link to first encryption/transmission device (TCM/ENC) 34. Second interface card 64 attaches to second common media 84 for main database 100.

FEC/TMD 34 is preferably a router. This device 34 encrypts the data stream and transports it across a common network with the receiving second encryption/transmission device (SEC/TMD 36). SEC/TMD 36 is preferably a virtual private network terminator. This encryption allows data to be securely passed between remote database 100 and local database 62

over public networks such as the Internet. Thus, the network management system of the present invention uses a specialized security transport and data transfer mechanism. In addition, these mechanisms are scaleable and adapted towards long-term trending.

Remote Site

Second Common Media 84 allows communication between all devices at the central location. Preferably, second common media is an ethernet system.

Remote site 42 comprises remote system agents, shown generally at 96, operating system agents shown generally at 98.

Remote main database 100 stores long term trending information about customer networks. Remote main database 100 also provides information for configuration module 52, data loader modules 46-50, transmission control module 60, AAIM 54, client GUI information, and client events.

Global security manager (GSM) 102 reviews security and intrusion patterns across company boundaries. This module more rapidly determines patterns and common attacks across the customer base and initiates alerts to the network security module (NSM) 108.

Advanced correlation module (ACM) 104 provides long-term correlation data information. It looks for patterns and trends that have occurred over longer periods of time and seeks to identify future problems.

Network configuration module (NCM) 106 provides a way to configure system agents for remote clients.

Network Security Monitor (NSM) 108. This device is monitored by staff to begin to

detect real-time attacks on customer networks.

Network management module (NMM) 110 performs the function of ...

Advanced Intelligence Device

Once information is provided from remote site 42 to second interface card 64 of advanced intelligence device 32, the information is sent to transmission control module 60. Upon receipt of the information, transmission control module 60 performs a look up to determine the format needed for data transmission, preferably wire data transmission. Once the format is known, transaction control module 60 in placed in communication with the appropriate application program interfaces and then sends the data to the appropriate interface.

Operation of the System

Figure 3 provides diagram of an agent configuration data flow; Figure 4 provides a diagram of an IDS collection data flow; Figure 5 provides a diagram of a trend performance collection data flow; and Figure 6 provides a diagram of a client graphical user interface data flow. These Figures are referred to during the discussion of the operation of the system as set forth below.

As shown in Figure 3, path 120 is energized when an administrator at an administrator console 122, which is located at a core network operations center, opens and connects to the client database, located within main database 100. Console 122 displays the current agent configuration information to the administrator. Next, the administrator makes changes to the agent configuration and database 100, which is updated with log and configuration information

according to path 124. Database 100 confirms the change and replicates the change to local client database 62, via the transaction coordinator 76, through path 126. Transaction coordinator 76 ensures that the data replication within local client database 62 is successful and transmits the data to local client database 62 when a stable network connection is detected, as shown in path 128.

Next, data is encrypted by second encryption/transmission device 36 and transferred across a wide area network, such as the Internet, through path 130. This transmitted data is received by first encryption/transmission device 34. The data is then transferred along path 132 to second interface card 64. It should be noted that the encryption at first encryption/ transmission device preferably occurs on site at the client location. Second interface card 64 passes the received data to the transaction control module 60, along path 134.

The transaction control module 60 processes the data, and formats the data in preparation for the agent update. Transaction control module 60 then prepares an information package for updating into local client database 62. For security purposes, this formatted information is first sent to security module 56 for logging along path 136. After the information passes through security module 56, the data is replicated to a local client database 62 via path 138.

Configuration module 52 is continually polling local client database 62 for agent changes using path 140. Upon detection of the replicated data, configuration module 52 retrieves the new values from local client database 62 along path 142. Configuration module 52 then processes the change in agent configuration, in accordance with the agent configuration dataflow shown in Figure 3, and transfers this information to security module 56 for logging, along path 144. After logging, security module 56 passes information along path 146 to transaction control module 60

for processing.

Transaction control module 60 sets up a transmission control protocol ("TCP") communication listener and transmits the newly-formatted request along path 148 to first interface card 44, which itself transmits the information to the remote operating system agent 88, along path 150. After receipt of the change request, remote operating system agent 88 processes the commands, executes a warm restart, and provides acknowledgment of the successful application of the commands. Such acknowledgment is provided along path 152 to first interface card 44. Acknowledgment is then passed by first interface card 44 to transaction control module 60, along path 154. Upon receipt of the acknowledgment, transaction control module 60 checks and determines whether a timeout has been reached. If the timeout has not been triggered, transaction control module 60 passes acknowledgment data to security module 56 along path 156 for logging. If the timeout has been triggered, the data is simply discarded, and the process for retrieving data restarts.

Security module 56 passes the acknowledgment data to configuration module 52 along path 158. Configuration module 52 uses path 160 to update local client database 62 with the acknowledgment. Local client database 62 replicates the data and provides information on this event through path 162 to security module 56.

Security module 56 passes the data replication to transaction control module 60 along path 164 for transmission. Transaction control module 60 passes the database replication information via path 166 to second interface card 64 for wide-area network/Internet transmission. Second interface card 64 passes information along path 168 to first encryption/transmission device 34, preferably a router.

First encryption/transmission device encrypts the data replication transaction, and sends the information along path 170, to second encryption/transmission device 36. Second encryption/transmission device decrypts the information, and passes this information along path 172 to transaction coordinator 76.

The transaction coordinator 76 passes the data replication information along path 174 to main database 100, to complete the final phase of agent configuration. Accordingly, this concludes one complete cycle of a change in agent configuration, from a data flow perspective.

To provide a more specific example of agent configuration, assume that a customer is monitoring server A (not shown) being monitored. The server, by default setting, sends out a utilization warning alert at a seventy percent (70%) utilization level, and a critical alert at a ninety percent (90%) utilization level. The customer decides that it would like a warning notification when the processor reaches sixty percent (60%) and would like a critical alert when the processor reaches a seventy-five percent (75%) utilization level. Based upon this desire to change the agent configuration parameters, the customer requests that the desired change be implemented. The change is input into an administration console and thus is input into main database 100. Upon receipt of this update, the data is replicated to local client database 62, in accordance with the transmission procedures discussed above. Configuration module 52 watches for changes in the data replicated to local client database 62. Upon recognition of the change in data, configuration module 52 communicates in accordance with the procedures set forth above through transaction control module 60 to client managed devices 66, and in this case, client server 70. Client server 70 receives the updated configuration information, updates its configuration, and restarts itself (reinitializes in Random Access Memory). Then, client server

70 replies to configuration module 52, in accordance with the procedures set forth above, that the change was successfully implemented. Configuration module 52 then communicates with local client database 62 and updates local client database 62. Next, this data is replicated to main database 100, in accordance with the procedures set forth above.

Figure 4 provides a data flow path diagram illustrating IDS collection. Cisco Netranger (recently renamed to Cisco Secure Intrusion Detection System) sensor 90 sends the event information along path 180 to first interface card 44. First interface card 44 sends the received data to transaction control module 60 using path 182. Transaction control module 60 also passes the unprocessed data along path 184 to security module 56 for logging. Security module 56 logs the event and sends confirmation of the logging to the transaction control module 60 along path 186. Transaction control module 60 sends the processed data to second interface card 64 using path 188 for transmission.

Data loader module 46 expects to receive information in a specific format to facilitate the calculation and manipulation of the data such as, for example, in calculations. Because the data sent by the client network is in an incorrect format, data loader module 46 is unable to process the raw data. Thus, one purpose for the placement of the transaction control module 60 between the data loader module 4 and the client network is to permit transaction control module 60 to process the received data by specifically formatting the data for the data loader module 46. In this way, properly formatted data is provided to data loader module 46, and data loader module 46 is able to apply the formulas it is required to execute.

Second interface card 64 uses path 190 to send the data to first encryption/transmission device 34 for transmission. First transmission encryption device encrypts the data and transmits

it across a wide area network path 192 to second transmission encryption device 36. Receiving and second transmission/encryption device 36 decrypts the data and forwards it using path 194 to Netranger director system 92. Netranger director system 92 uses path 196 to update main database 100 with event data.

As is evident from the data flow diagram in Figures 3, 4 and 5, all data flows are logged through the security module 56. The security module logs date, time, initiating module, receiving module, and a short description of the event. The actual data passed through security module 56 is not retained in memory under normal settings, to avoid memory capacity issues. However, it is possible to reset the logging parameters to include a complete capture of the data flow, which could be especially helpful in troubleshooting.

Figure 5 illustrates a data flow diagram detailing the collection of trend performance information. First data loader module 46 is loaded into memory from local client database 62 using path 200. Data loader module 46 initiates the set up of data collection services. Information on the data to be collected is passed along path 202 to security module 56 for logging. After logging, information on the data to be collected is passed along path 204 to transaction control module 60.

Upon receipt of the information on the data to be collected, transaction control module 60 determines what service data extraction to initiate. In addition, transaction control module 60 sets up a listener for incoming SYSLOG information from firewall 95. Once this determination is made, a structured packet of information is created by firewall 95. Next, transaction control module 60 uses path 206 to send the now structured packet of information to first interface card 44 for transmission on the client network, first common media 40.

First interface card 44 then uses path 208 and path 210 to poll router 93 and server 94, respectively. The polling process occurs on scheduled intervals. The polling process is a standard SNMP get-next request. The polling is initiated by transaction control module 60.

Path 212 is an example of a SYSLOG feed. SYSLOG information is regularly transmitted from firewall 95 through path 212 to first interface card 44, and then through path 214 to transaction control module 60 which has set up a listener for the incoming information.

At the same time that the SYSLOG operations, router 93 replies to the SNMP poll by transmitting data in standard SNMP format via path 216 to first interface card 44, and then through path 214 to transaction control module 60. Similarly, server 94 replies to the SNMP poll by transmitting data in standard SNMP format via path 218 to first interface card 44, and then through path 214 to transaction control module 60. Therefore, even though the data collection protocols are completely unrelated, both SYSLOG and SNMP data protocols are being received and processed by transaction control module 60.

Transaction control module 60 converts the format of the data received to a variable name and/or variable value. For example, the data could be received in an SNMP or a SYSLOG format. Both data formats are converted to variable name and/or variable value formats. Then transaction control module 60 uses path 220 to pass the converted data format to security module 56 for logging. Security module 56 logs the data and passes the information to data loader module 46 using path 222.

Data loader module 46 processes the information. Specifically, data loader module 46 checks and determines whether all of the information received is required and correct. In addition, data loader module 46 applies the formula for consolidation and loads this information

using path 224 into local client database 62.

Local client database 62 begins replicating the information received from data loader module 46. Once the replication process is initiated, local client database 62 uses path 228 to initiate a request to security module 56 for logging. Security module 56 logs the replication information and passes it through path 230 to transaction control module 60 for transmission to main database 100. To accomplish this, transaction control module 60 directs over path 232 the replication parameter information to second interface card 64. Second interface card 64 sends data over path 234 to first encryption/transmission device 34 where the replication parameter information is packetized and encrypted for transmission across a wide area network 236 such as the internet.

Upon receipt of the encrypted transmission, second encryption/transmission device 36 decrypts the replication parameter information and passes it using path 238 to transaction processor 76. Transaction processor 76 unpacketizes the information and loads the data via path 240 into main database 100. At this point, the replication process which began with local client db b2 is complete.

The interaction between DLM 46 and transaction control module 60 is best illustrated in the following example. A customer would like to view the utilization information of the Ethernet port of his or her routers. Thus, data loader module 46 must be directed to Received LAN Utilization. In this case, the following information is placed in a block of code:

```
                DLM Name:  Received LAN Utilization (10mb Full
duplex Ethernet)

                DLM Variables:  5
                DLM Method: SNMPv2 Get-Next
```

```
                Formula:  Utilization = Delta (IfInUcastpkts +
IfInNUcastpkts+IfinErrors) * 16 + Delta (IfinOctets)*.8
                                                Delta
(sysUptime/100)*10,000
                Host1 Name:  Server1
                Host1 IP address:  10.1.50.1
                Method Var: 1
                Interval: 300

                Host2 Name:  Server2
                Host2 IP Address: 10.1.50.2
                Method Var: 2
                Interval:  300

                Variable1:  IfinUcastPkts
                Value1:
                Variable2:  IfInNUcastpkts
                Value 2:
                Variable3:  IfinErrors
                Value3:
                Variable4:  IfinOctets
                Value4:
                Variable5:  sysUptime
                Value5:
                DataLoading_Procedure: SQL_Load Script
                Temp_storage Procedure:  SQL_Working Script
```

As is evident, the DLM 46 has very specific information needs. DLM 46 cannot process raw data that is in SNMP format. As explained above, DLM 46 sends a request for data to the transaction control module 60 based on these needs. The request for data is a variable/value request (i.e. ifinucastpkts, ifinnucastpkts, etc.) and an SNMP method is specified (here SNMP version 2) for how to get this information from the client network. This information is sent to transaction control module 60. Transaction control module 60 first looks at the method and determines that this is an SNMPv2 Get-next method.

Based on its knowledge of the SNMP protocol, transaction control module 60 prepares an SNMP request for the variables identified and sends it to the named host on the client network. (In this case 10.1.50.2). Thus, transaction control module 60 determines the object identifiers

associated with the formula used by DLM 46 as set forth below.

Standard OIDs associated with this formula:

	OID for Formulas
SysUptime	.1.3.6.1.2.1.1.3
IfInOctets	1.3.6.1.2.1.2.2.1.10.instance
IfInUcastPkts	.1.3.6.1.2.1.2.2.1.11.instance
IfInNUcastPkts	.1.3.6.1.2.1.2.2.1.12.instance
IfinErrors	.1.3.6.1.2.1.2.2.1.14.instance

It is recognized that IfInOctets and the other terms directly above are well known in the art according to SNMP standards.

Received Utilization =
[Delta(IfinUcastPkts+IfinNUcastPkts+ifInErrors) * 16 + Delta(IfinOctets) * .8] divided by
[Delta(sysUptime/100) * 10,000]

The Received Utilization formula is well known, and is used in order to make the units work properly. Thus, the multiplier of 16 is due to the fact that the octets are being converted to bytes, and that there is a packet delay factor.

The transaction control module 60 request that has been translated to account for the DLM 46 request, the specified method, and the identification of information, goes to the SNMP agent of router 93. The SNMP agent of router 93 performs standard SNMP data collection techniques and then ends the reply back to transaction control module 60 through the first interface card 44. Upon receipt of the reply transaction control module 60 examines that sysuptime, IfinUcastPkts, IfInNUcastpkts, IfinErrors ,and IfinOctets have valid values. The TCM then prepares a reply to the initiating DLM in the format of variable/value:

```
(sysuptime,61781915,ifInUcastPkts,309698,ifInOctets,249595928,ifI
nUcas
 tPkts,309698,ifInNUcastPkts,0,ifInErrors,143126)
```

Thus, DLM 46 receives only the data that it has requested and processes the information according to the formula, while transaction control module 60 eliminates problems associated with translation of variables and standards.

DLM 46 now uses the temp storage procedure to temporarily store this data in local database, this is done so a delta can be computed. Upon receipt of a second reply from transaction control module 60, data loader module 46 applies the formula and loads the result into local client database 62. This process continues with transaction control module 60 making the request to router 93 at the required time interval.

As the example above covered only Received LAN Utilization, it is fully contemplated by the present invention that many different data loader modules 46-50 may be employed, and the invention is not limited to any particular number of data loader modules. For example, a Sent LAN Utilization may be employed. Other subjects for data loader module coverage include the handling of various alerts and warnings, and any other performance data. It is specifically noted that the data loader modules of the present invention are not limited to the use of SNMP methods. This lack of limitation is because most, if not all, customers will have a firewall. Firewalls generally have business rules that allow or deny traffic originating outside the network from entering into the network. By and large, firewall vendors have picked SYSLOG (not SNMP) as the method to notify management systems of policy violations and system status. To handle this firewall notification, a SYSLOG data loader module is created. This data loader module informs the transaction control module 60 to set up a user datagram protocol (UDP)

listener on port 514. Additional information regarding the UDP is available on the Internet at http://www.cis.ohio-state.edu/rfc/rfc0768.txt. As is evident in this standard, information generated by the SYSLOG method is largely a textual description with severity and source information. Because UDP is a connectionless protocol, SYSLOG messages are only sent to the listener. Accordingly, no confirmation of receipt of data is returned to the firewall. The listener, transaction control module 60, forwards the received information to the SYSLOG data loader module where the information is processed and then loaded into the local database in accordance with the communication procedures set forth above. Typical data that is delivered from a firewall is well known in the art and can be found on the Internet at the following location: http://www.sisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v52/syslog/pixemsgs.htm.

In addition to SNMP and SYSLOG, other network data collection methods include, but are not limited to, Common Information Method ("CIM"), Web Based Enterprise Management ("WBEM"), Desktop Management Interface ("DMI").

Figure 6 is a data flow diagram depicting the operation of the client's graphic user interface. Client machine with Java shell 67 initiates a connection 250 to network management system 20 by communicating with first interface card 44. First interface card 44 receives a request for access and passes it to transaction control module 60 via path 252. Transaction control module 60 receives the request, and uses path 254 to forward the request for access to security module 56.

Security module 56 prepares a challenge for user identification information and forwards the challenge via path 256 to transaction control module 60 for transmission to client machine 67 via path 258 to first interface card 44 and path 260 to client machine 67.

Client machine 67 then responds with a challenge phrase answer transmitted via path 262 to first interface card 44 and thence via path 264 to transaction control module 60. Transaction control module 60 receives the challenge answer and passes it along path 266 to security module 56 for logging and verification. Upon the verification of the user identification, security module 56 permits access to graphical user interface module 69 via path 268. Graphical user interface module 69 uses path 270 to retrieve objects from local client database 62. Local client database 62 retrieves the user interface objects and sends them along path 272 to graphical user interface module 69 for transmission to the client machine 67.

There are a variety of user interface objects that may be requested. Depending on the user interface object requested, information is retrieved and sent along differing paths. Specifically, if the user has requested trend, intrusion detection system ("IDS") or event information, the local client database 62 must obtain this information from main database 100. To do this, local client database 62 uses path 274 to pass the request for information to transaction control module 60. Transaction control module 60 uses path 276 to utilize second interface card 64 to transmit along path 278 the request to first encryption/transmission device 34. The request is encrypted by first encryption/transmission device 34 and transmitted along public network path 280 to second encryption/transmission device 36. Second encryption/transmission device 36 decrypts the request and sends the request along path 282 to transaction processor 76. Transaction processor 76 uses path 284 to transmit the request to main database 100.

Main database 100 processes the request, retrieves the requested information, and sends the requested data out along path 286 to transaction processor 76 which itself forwards the data to second encryption/transmission device 36 along path 288. Second encryption/transmission

device 36 encrypts the data and transmits the data over public network path 290 to first encryption/transmission device 34. First encryption/transmission device 34 decrypts the data and sends the decrypted data along path 292 to second interface card 64. Second interface card 64 uses path 294 to transmit the data to transaction control module 60. Transaction control module 60 converts the data and sends it along path 296 to security module 56. Security module 56 logs receipt of the data and forwards the data to graphical user interface module 69 along path 298.

At this point, graphical user interface module 69 processes this data and prepares the data for delivery to client machine 67. Specifically, graphical user interface module 69 uses path 300 to transmit information to security module 56, which logs the data and uses path 302 to forward the data to transaction control module 60. Transaction control module 60 sends the data along path 304 to first interface card 44, which transmits the data across Transmission Control Protocol ("TCP") connection 306. This concludes the data flow paths which take place when a user requests trend, IDS, event data or any data residing at main database 100.

If the user has not requested trend, IDS, event data, or any data residing at main database 100, graphical user interface module 69 passes objects along path 308 to security module 56 for logging. Security module 56 logs and passes objects to transaction control module 60 via path 310. Transaction control module 60 packetizes the data objects and transmits these packets along path 312 to first interface card 44. First interface card 44 transmits these packets to client machine 67 along path 314. At this point, a constant connection is established between first interface card 44 and client machine with Java shell 67, as a user navigates the interface. Requests by the user for relevant data are sent over this path 314 to graphical user interface module 69. In addition, as network information is generated, graphical user interface module 69

sends updated information to the client display located at client machine 67 via path 308.

Turning to Figure 7, an explanation of the operation of correlation module 58 will commence. Trend performance is stored in local client database 62, in accordance with the trend performance collection procedures discussed with respect to Figure 5. In addition, the alert, event and performance information produced pursuant to the trend performance data capture is sent to correlation module 58. Intrusion detection information is provided to main database 100 in accordance with the intrusion detection procedures set forth in association with Figure 4. The intrusion detection information is also provided to correlation module 58. Accordingly, correlation module 58 has access to intrusion detection information, performance information and alert information. Correlation module 58 receives instructions from AAIM 54 (in accordance with the transmission procedures used throughout these examples) on how to correlate information. Correlation module 58 then applies these instructions to the data to calculate and determine correlations.

Correlations may take different forms. One correlation is the correlation of a performance spike on interface utilization combined with an intrusion detection alert. These two events may be correlated to prompt an alert message from correlation module 58 of a potential or actual hacking attack, depending on the strength of the correlation.

Another correlation to be performed by correlation module 58 is between a peak on central processing unit utilization with a low memory warning, coupled with an application failure. These events may also trigger an alert from correlation module 58.

Yet another correlation could be performed by correlation module 58 on a peak on central processing unit utilization without a low memory warning, coupled with an application failure.

These events may also trigger an alert from correlation module 58.

It is the intention of the present invention that correlation module 58 derive its correlation function from AAIM 54. Specifically, it is the intention of the present invention to derive a benefit from serving multiple client networks. Across multiple client networks, performance, event and intrusion data may be correlated using advanced correlation module 104 to provide long-term correlation data information. Advanced correlation module 104 looks for patterns and trends that have occurred over longer periods of time and seeks to identify future problems. Once trends or problems are identified, modification to configuration module 58 instructions are stored in main database 100. Because correlation module 58 regularly polls AAIM 54 for new information, in accordance with the communication procedures set forth above, configuration module 58 will receive the updated instructions rapidly.

It is emphasized that the present invention provides a superior, secure means of providing service to multiple client networks. In the past, network service providers would simply connect directly to the client network. This direct connection creates security issues where multiple clients are involved. This is because one client may reach a different client by using the service provider as a switch. The present invention eliminates this danger by interposing an advanced intelligence device 32 to serve as a buffer between any client network and the service provider. Further, the additional security also enhances the ability of the service provider to extract performance and intrusion detection information securely, confidentially and anonymously, while sharing the benefits of the experiences across multiple client networks with all client networks.

We now turn to Figures 8-18. These figures reflect the appearance of graphical user interface (client machine with Java shell) 67. As is illustrated in the different interface screens

provided in these Figures, an iconic and instinctive approach for providing network-related information to the client has been taken. On the left side of each screen, an index of eight screen areas is provided. Figure 8 illustrates the result when the "map" button on the left side is clicked with a mouse. If the firewall icon is clicked, a filter is applied to the bottom portion of the screen display. It is noted that intrusion detection, firewall, and DMZ icons require security administrator privileges prior to the provision of a filter. The headquarters icon changes color based on the status of objects. The link between headquarters and the Miami location is animated and changes color based upon predefined variations. For example, a critical link capacity will change the link color to red. Adjacent the link, there is also provided a Current versus Trend View allows an easy wide area network overview, which is updated over regular intervals, such as five minute intervals.

Double clicking on an icon object explodes the object into a detailed site view. Clicking anywhere in the background applies a general filter. An overview of events occurring throughout the network from traps and events generated by agents is also provided.

Similarly, with respect to Figure 9, the same principles set forth in the explanation of Figure 8 are similarly reproduced with respect to Figures 9-18. With respect to Figure 9, specifically, and Ethernet Bar is provided which is static and is not animated. However, each server link attached to the Ethernet Bart is animated and changes color based upon status and utilization levels.

With respect to Figure 10, double clicking on the memory icon brings up a listing of top ten (10) memory-utilizing system processes.

Figure 11 provides information on data derived from trend performance collection data, as discussed above in association with Figure 5.

In Figure 12, clicking on Tree items, filters, the list to the right of the Tree item. The Tree

leaves change color based upon the status of the items included below each leaf.

Figure 13 provides the user with displays that provide summaries of utilization, Again, clicking on any icon will provide more detailed information, as discussed in connection with the exploded object concept in Figure 8.

Figure 15 displays various sensors which are categorized as either private or public. Public sensors are typically internet-positioned sensors. Private sensors are typically sensors which are accessed by clients.

Figure 16 illustrates the user interface when it is displaying the results of the operation of correlation modules, 58 and 104.

Figure 17 illustrates various reports which may be selected for further details.

Figure 18 illustrates the means for changing agent configuration settings. Once changes in agent configurations are requested, the agent configuration is changed, as discussed in greater detail and the discussion accompanying Figure 3.

In view of the foregoing, it will be seen that the several advantages of the invention are achieved and attained.

The embodiments were chosen and described in order to best explain the principles of the invention and its practical application to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated.

As various modifications could be made in the constructions and methods herein described and illustrated without departing from the scope of the invention, it is intended that all matter contained in the foregoing description or shown in the accompanying drawings shall be interpreted

as illustrative rather than limiting. For example, advanced intelligence device 32 may be located off customer premises, but may still be in communication with the client's existing network and extracting data therefrom. In another example, first and second interface cards, 44 and 64 respectively, are communications interfaces, and are not limited to any particular "card" structure or geometry. Thus, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims appended hereto and their equivalents.

What is Claimed Is:

1. A method of managing a network comprising:

connecting an advanced intelligence device to an existing network;

connecting a network operations center to said advanced intelligence device;

providing an advanced intelligence device with a plurality of data loader modules, a configuration module, an advance artificial intelligence module, a correlation module, a security module, a transmission control module, a first interface for communicating with the existing network, a second interface for communicating with said network operations center;

providing said network operations center with a main database, a global security module, an advanced correlation module, a network configuration module, and a network security monitor;

wherein said network operations center is connected to said advanced intelligence device via a transaction processor and a router;

using said advanced intelligence device to extract performance data from the existing network; and

processing the data in at least one of said advanced intelligence device and said network operations center by correlating the data to identify potential network attacks.

2. A method of managing a network according to claim 1, further comprising:

using said network operations center to control the extraction of data from the existing network by said advanced intelligence device.

3. A method of managing a network according to claim 1, further comprising:

using said security module to log data transfers between said modules disposed within said advanced intelligence device.

4. A method of managing a network according to claim 1, further comprising:

using said security module to log data coming into said advanced intelligence device.

5. A method of managing a network according to claim 1, further comprising:

using said security module to log data going out of said advanced intelligence device.

6. An advanced intelligence device comprising:

a local database for storing information about agent configuration,

a data loader module in communication with said local database;

an advanced artificial intelligence module in communication with said local database;

a correlation module in communication with said advanced artificial intelligence module;

a security module in communication with said data loader module;

a transmission control module in communication with said security module;

a correlation module in communication with said local database;

a transmission control module in communication with said security module;

a first interface card in communication with said transmission control module, said first interface being adapted to communicate with the existing network to transmit and receive data;

a second interface card in communication with said transmission control module;

wherein said local database stores software code for accessing by said data loader module, and wherein said data loader module transmits a request for information that is passed through said security module to said transmission control module and said data loader module receives the requested information from said transmission control module through said security module;

wherein said transmission control module processes requests for information from said data loader module, creates and transmits a request for information through said first interface device, and receives and processes the requested information prior to transmittal of the information to said data loader module.

7. A method of operating a data loader module comprising the steps of:

storing mathematical formulas for calculating and creating useful data from the collected data;

instructing a transmission control module on what types of data to retrieve from a managed device;

providing instructions to said transmission control module on how to obtain that data;

receiving data from said transmission control module;

modifying the data in accordance with the stored mathematical formulas; and

delivering modified data to a local database.

8. A method of operating an advanced artificial intelligence module comprising the steps of:

reading data being collected by a plurality data loader modules;

reading correlated data being transmitted from a local database to a data correlation modules;

providing probability and statistical information about overall system events, such events including security, performance, and error conditions;

evaluating the data to determine the existence of patterns relating to network problem sources; and

loading information into said local database for future comparisons.

9. The method of claim 8, further comprising:

receiving information from a remote database that permits said evaluation to be modified.

10. A method of operating transmission control module comprising the steps of:

receiving a request to collect data from a specific module;

storing information about what procedures said specific module will use to collect the data;

storing information about what data said specific module is requesting;

instructing specific interfaces to obtain raw data using a module specific method;

receiving raw data from said specific interfaces;

processing the raw data to produce the information requested by said specific module;

transmitting the requested information to said specific module.

11. A method of operating a global advanced correlation module comprising the steps of:

collecting information on performance and intrusion detection from multiple client networks;

securely transmitting said information to said global advanced correlation module;

storing said information in a database in said global advanced correlation module;

searching said database for patterns of potential intrusion into any one of said multiple client networks.

12. The method of claim 11, further comprising:

communicating the discovery of a pattern of potential intrusion to an advanced intelligent device.

13. A method of extracting information from a network comprising:

transferring a database object from a location at a first network to a local database on said first network, which local database is physically located at a second network, wherein said database object is a data loader module;

connecting said first network to said second network with an interface;

initializing said data loader module from said local database as a first software application in random access memory;

transmitting a request for information from said first network to said second network;

transmitting the requested information from said second network to said first network; and

processing the received requested information within the first network;

loading the processed information into said local database in order to use the information.

14. The method according to claim 13, wherein the request for information comprises the variables necessary to compute network component utilization, and wherein the step of processing the information comprises the step of calculating network component utilization.

15. A method of managing a network comprising:

connecting an advanced intelligence device to an existing network;

connecting a network operations center to said advanced intelligence device;

channeling through said advanced intelligence device and logging within said advanced intelligence device all flows of data between said network operations center and said advanced intelligence device; and

channeling through said advanced intelligence device and logging within said advanced intelligence device all flows of data between said existing network and said advanced intelligence device.

16. A method of managing a network, in accordance with claim 15, further comprising:

correlating data from said existing network, said correlation being performed by said advanced intelligence device.

17. A method of managing a network, in accordance with claim 15, further comprising:

correlating data from said existing network, said correlation being performed by said

network operations center.

18. A method of configuring the extraction of data from an agent compromising:

changing an agent configuration and a main database;

transmitting and replicating this change to a local client database;

polling said local client database with a configuration module, and detecting a change in the agent configuration;

processing the change in agent configuration and passing the information to a transaction control module;

setting up a newly formatted request by said transaction control module, and transmitting the request, to said agent;

providing acknowledgment of the newly formatted request from said agent to said transaction control module;

passing said acknowledgment from said transaction control module to said configuration module;

updating said local client database from said configuration module; and

replicating the acknowledgment in said local database to said main database.

19. The method according to claim 18, wherein the step of passing said acknowledgment from said transaction control module to said configuration module compromises:

passing said acknowledgment from said transaction control module to a security module;

logging the acknowledgment within said security module; and

passing said acknowledgment from said security module to said configuration module.

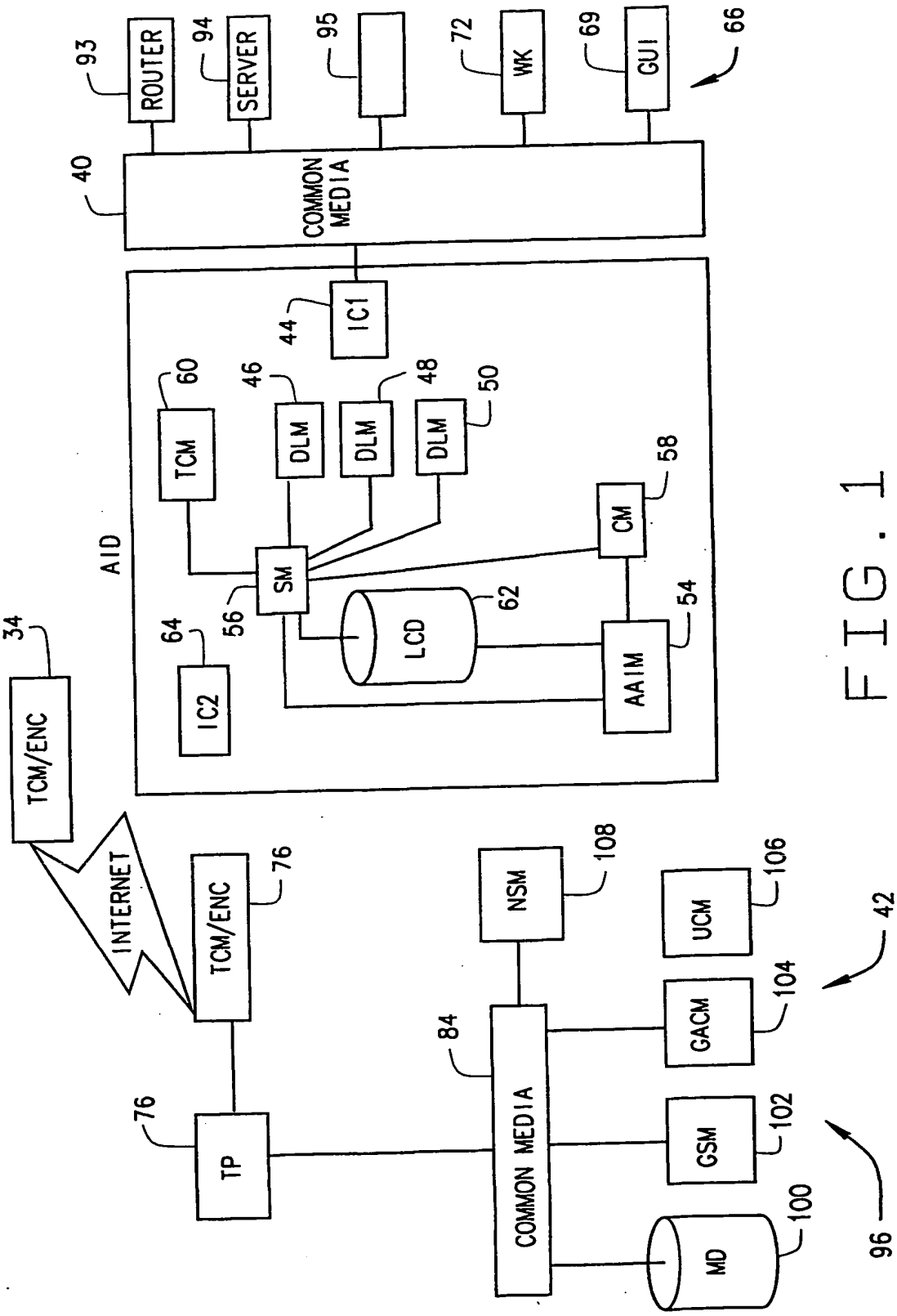

93
ROUTER
94
SERVER
95
72
WK
69
GUI
66
40
COMMON MEDIA
44
IC1
60
TCM
46
DLM
48
DLM
50
DLM
58
CM
AID
SM
56
LCD
62
64
IC2
54
AAIM
34
TCM/ENC
INTERNET
76
TCM/ENC
108
NSM
106
UCM
42
84
GACM
104
76
TP
COMMON MEDIA
GSM
102
MD
100
96

FIG. 1

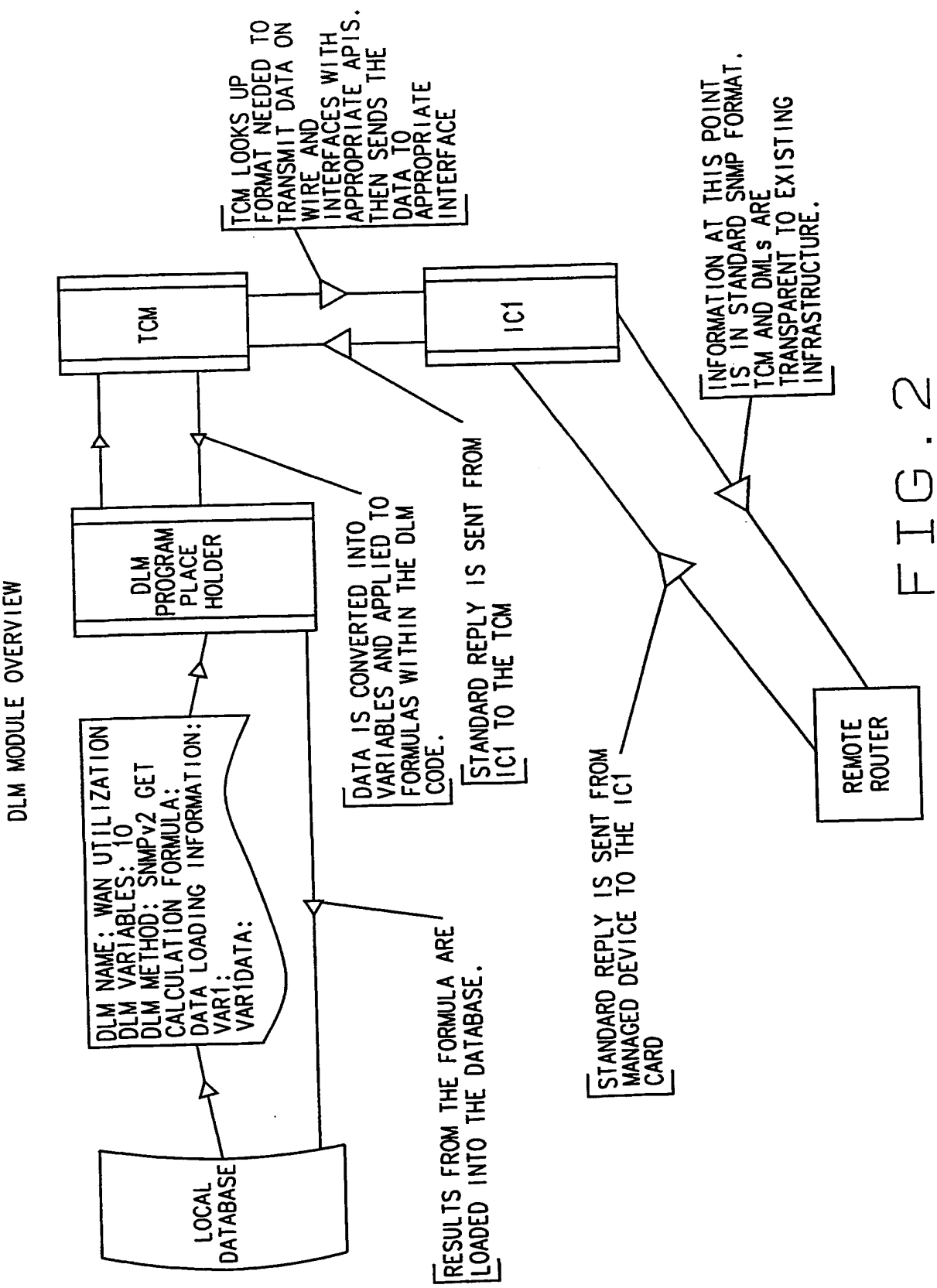


FIG. 2

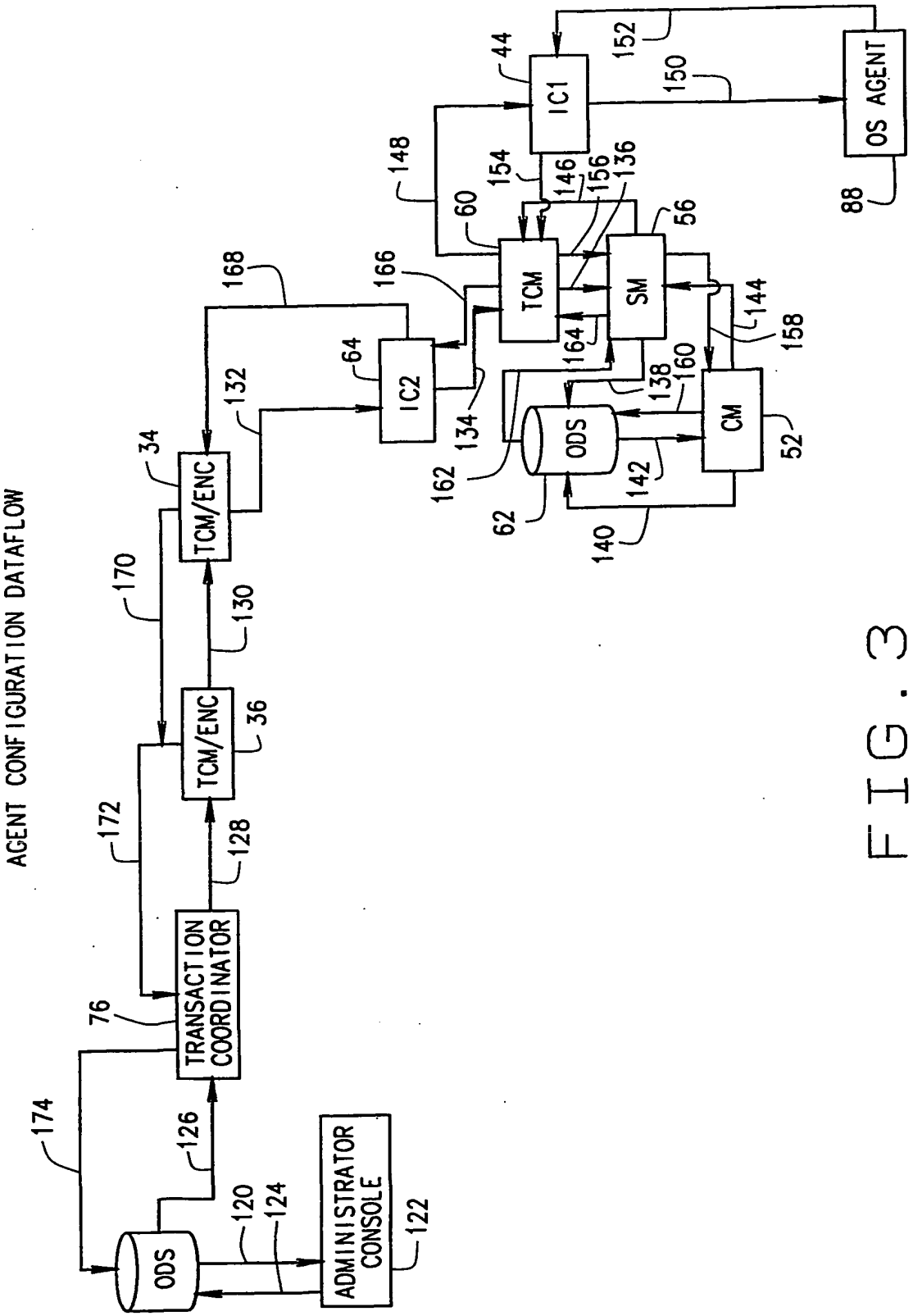


FIG. 3

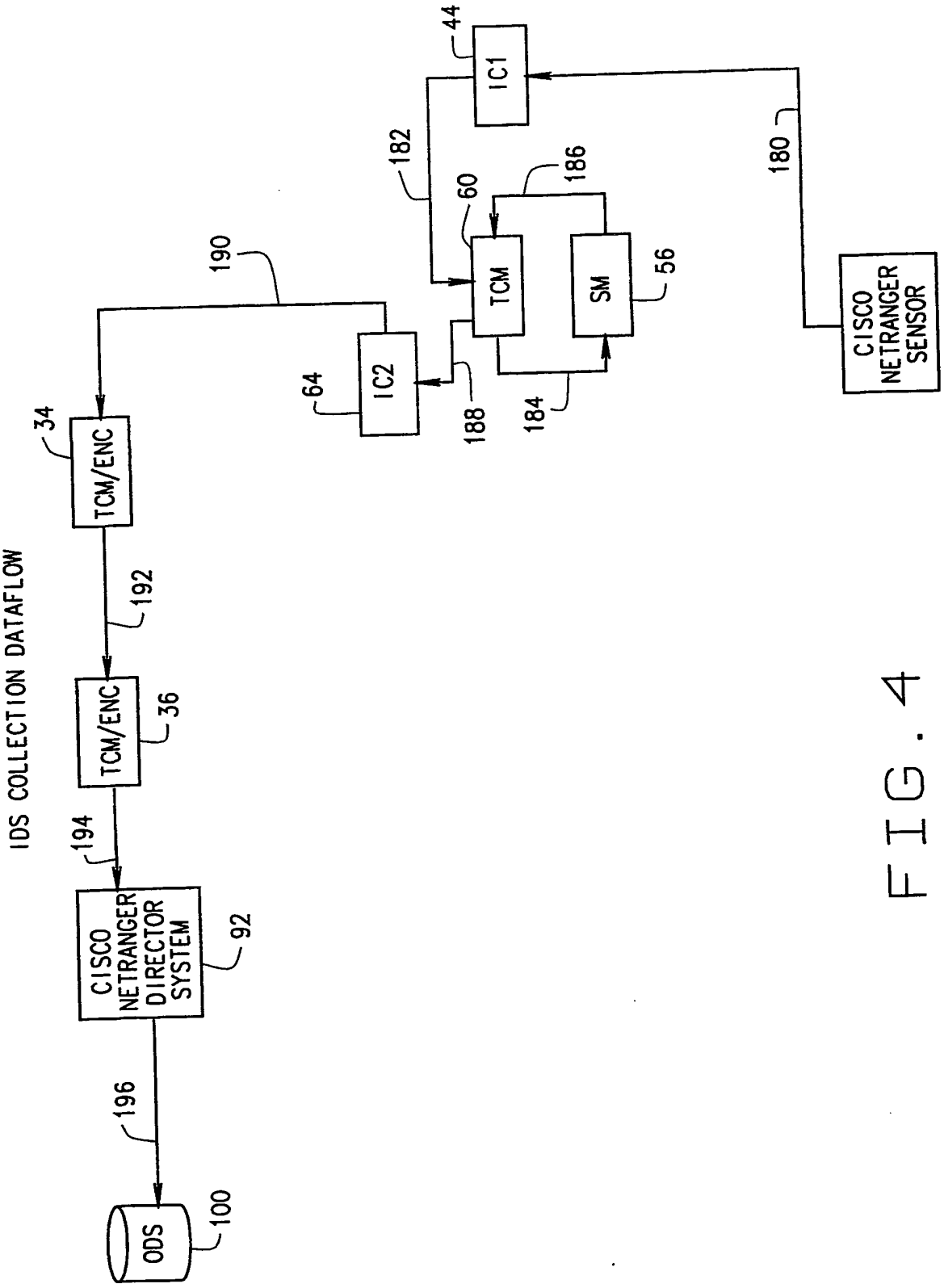

IDS COLLECTION DATAFLOW
TCM/ENC
34
192
TCM/ENC
36
194
CISCO NETRANGER DIRECTOR SYSTEM
92
196
ODS
100
190
IC2
64
188
184
TCM
60
SM
56
182
186
IC1
44
180
CISCO NETRANGER SENSOR

FIG. 4

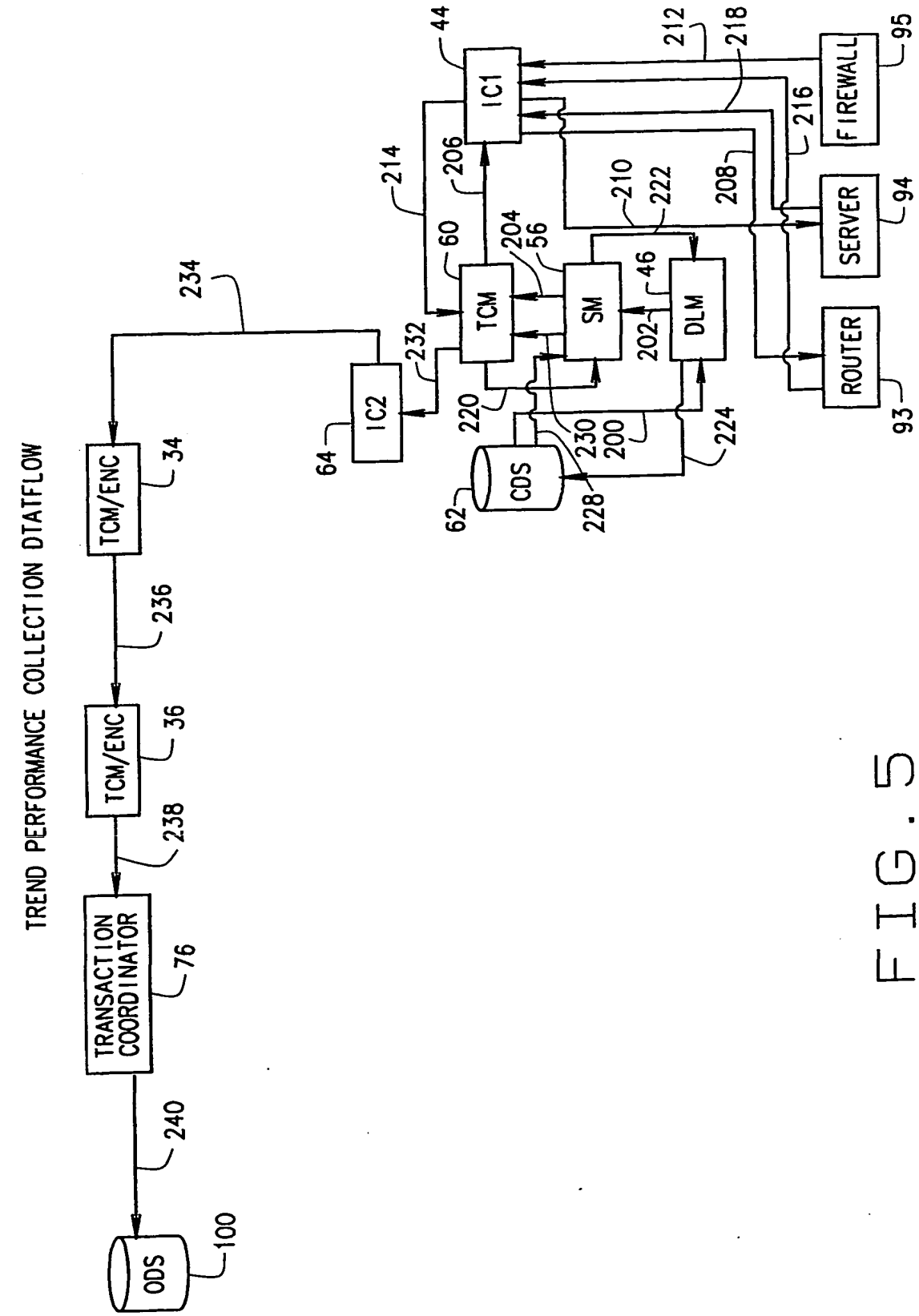


FIG. 5

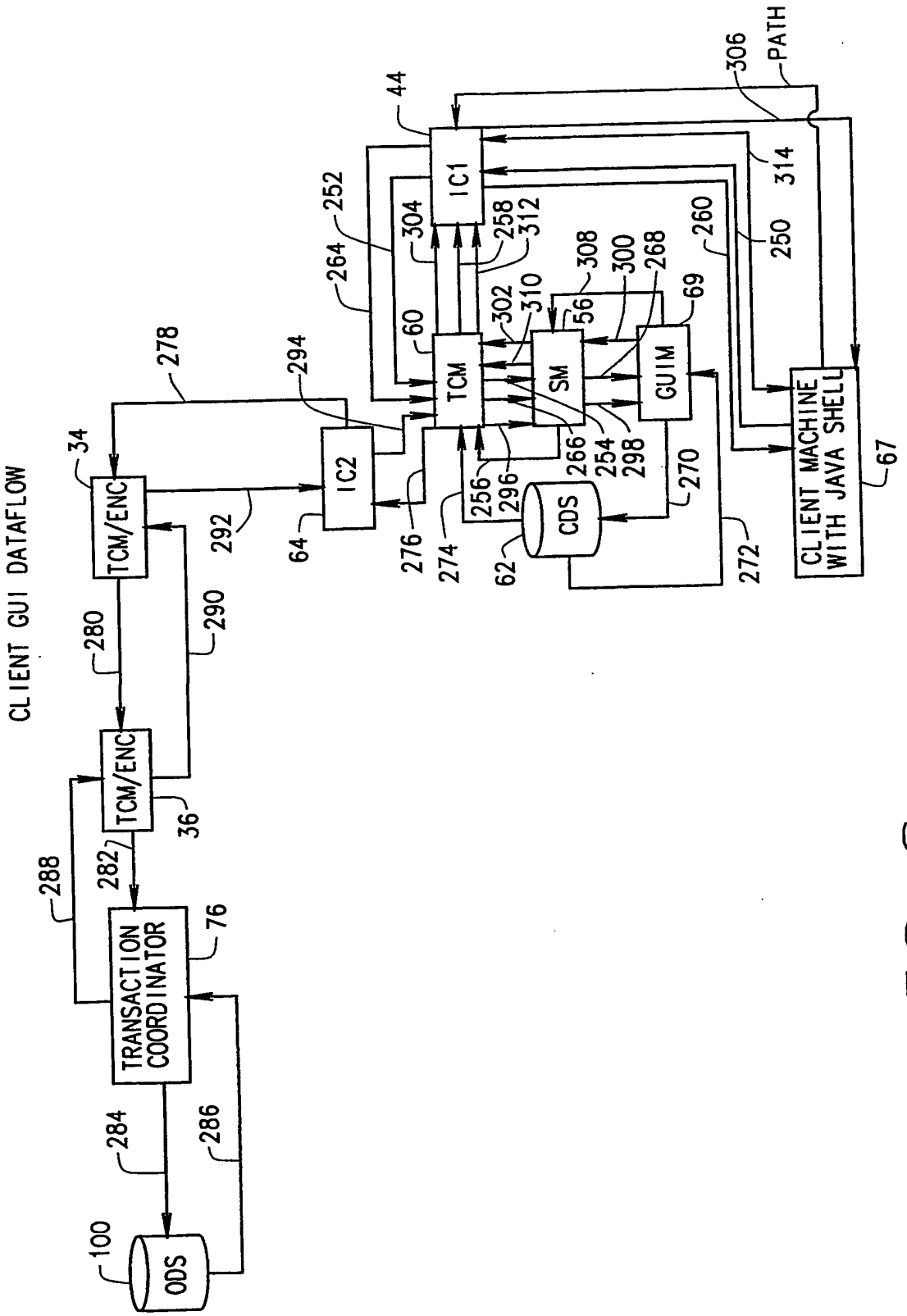

CLIENT GUI DATAFLOW
TCM/ENC
TCM/ENC
TRANSACTION COORDINATOR
ODS
IC2
IC1
TCM
SM
GUIM
CDS
CLIENT MACHINE WITH JAVA SHELL
PATH
34
36
44
56
60
62
64
67
69
76
100
250
252
254
256
258
260
264
266
268
270
272
274
276
278
280
282
284
286
288
290
292
294
296
298
300
302
304
306
308
310
312
314

FIG. 6

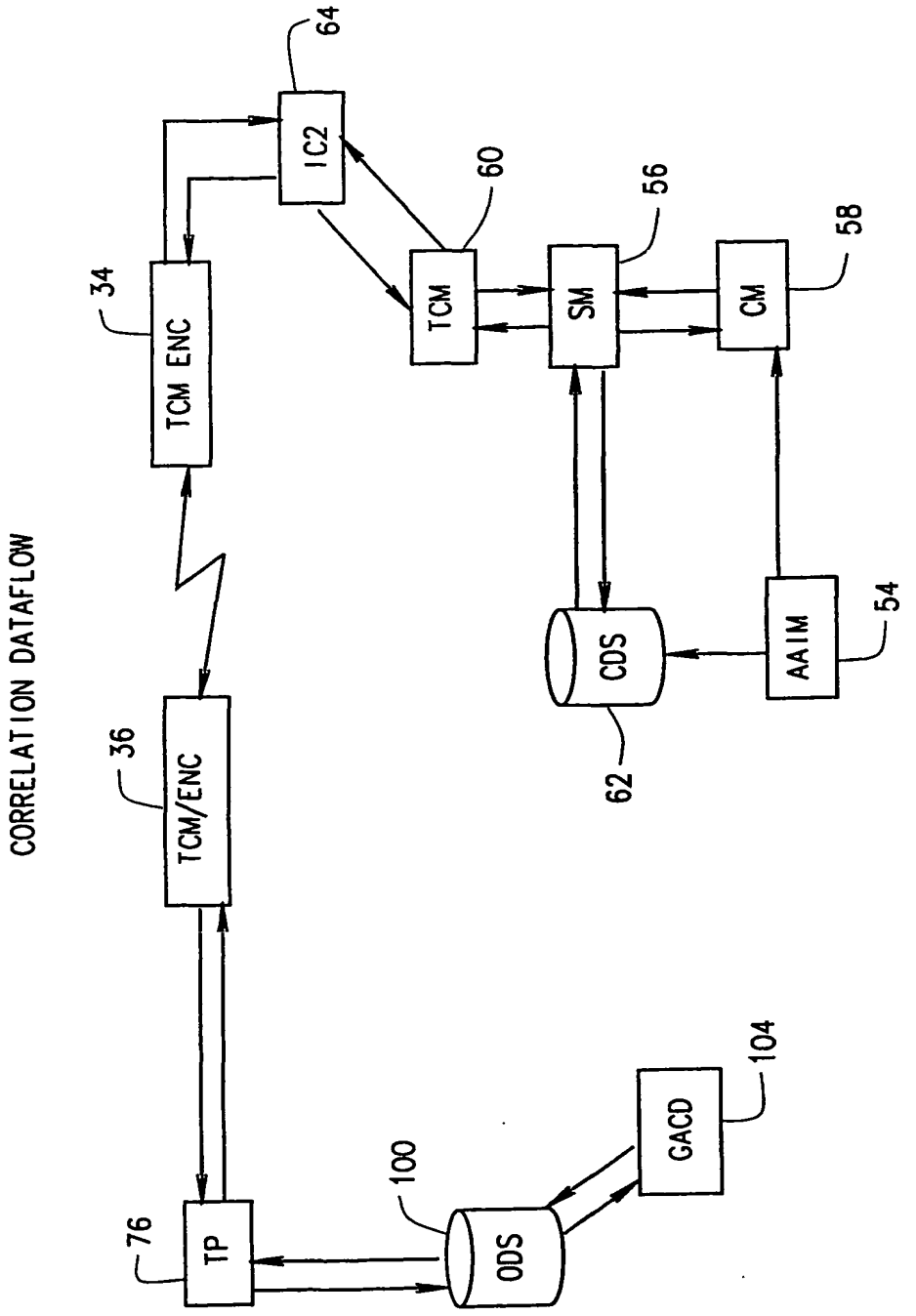


FIG. 7

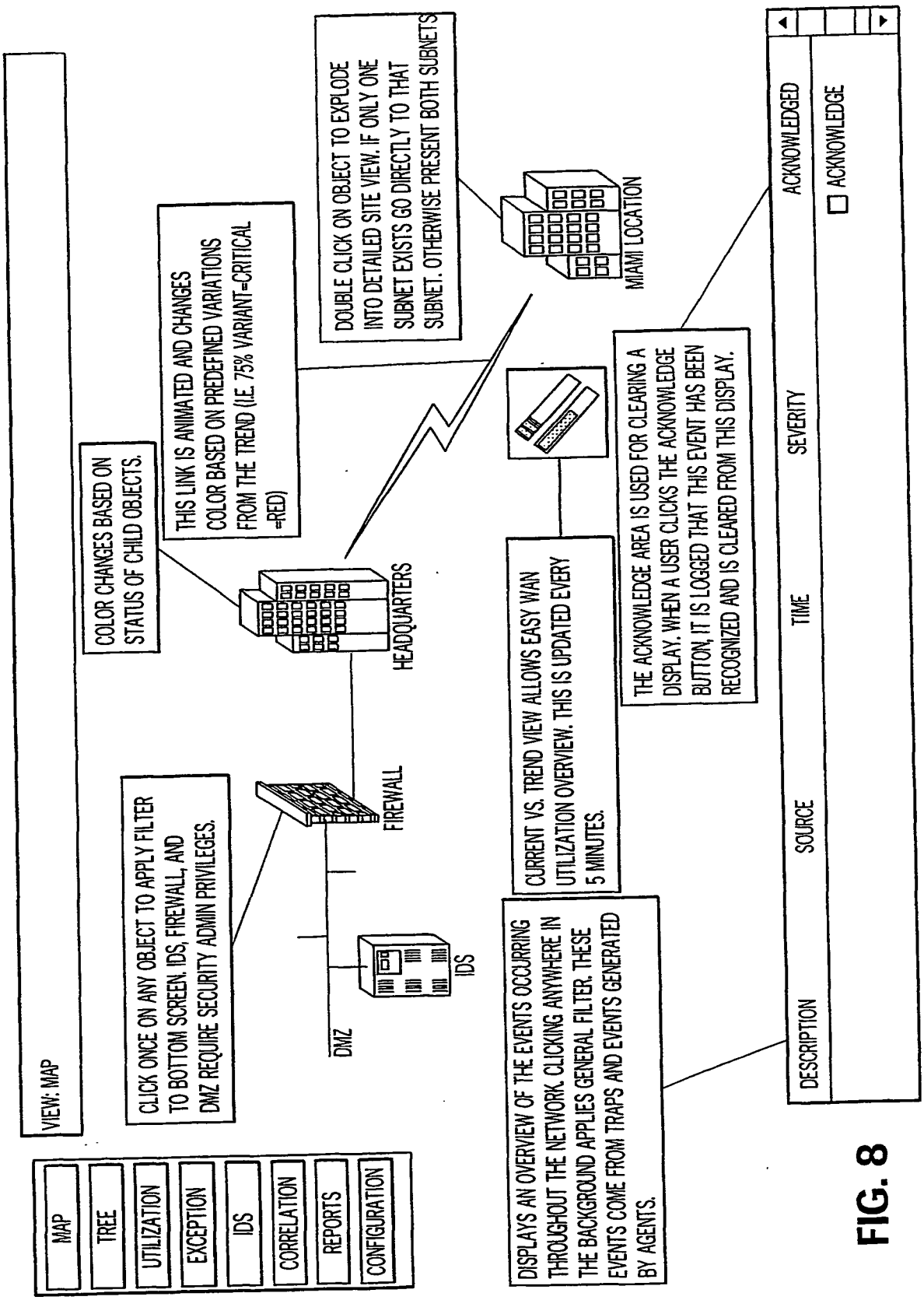


FIG. 8

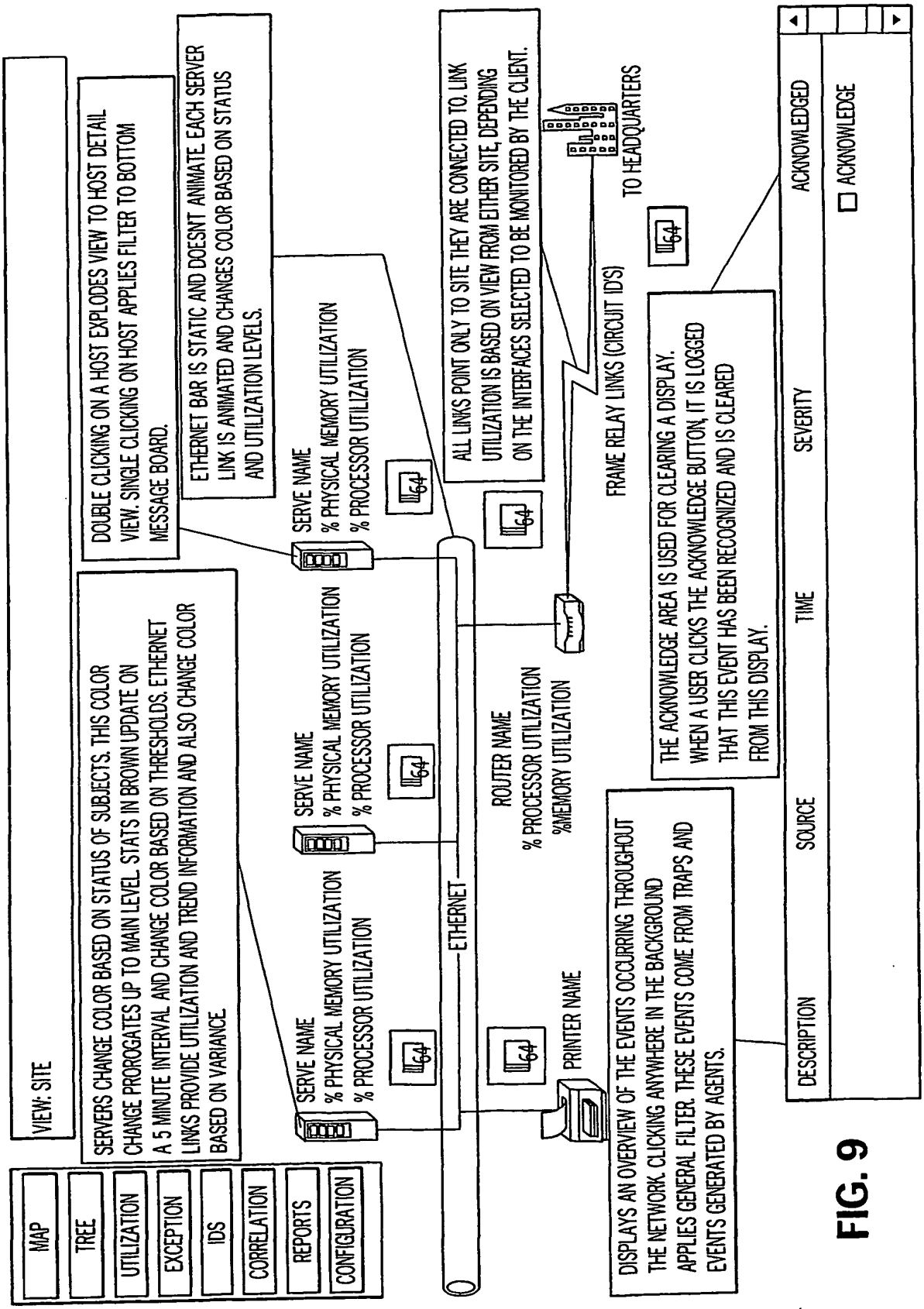


FIG. 9

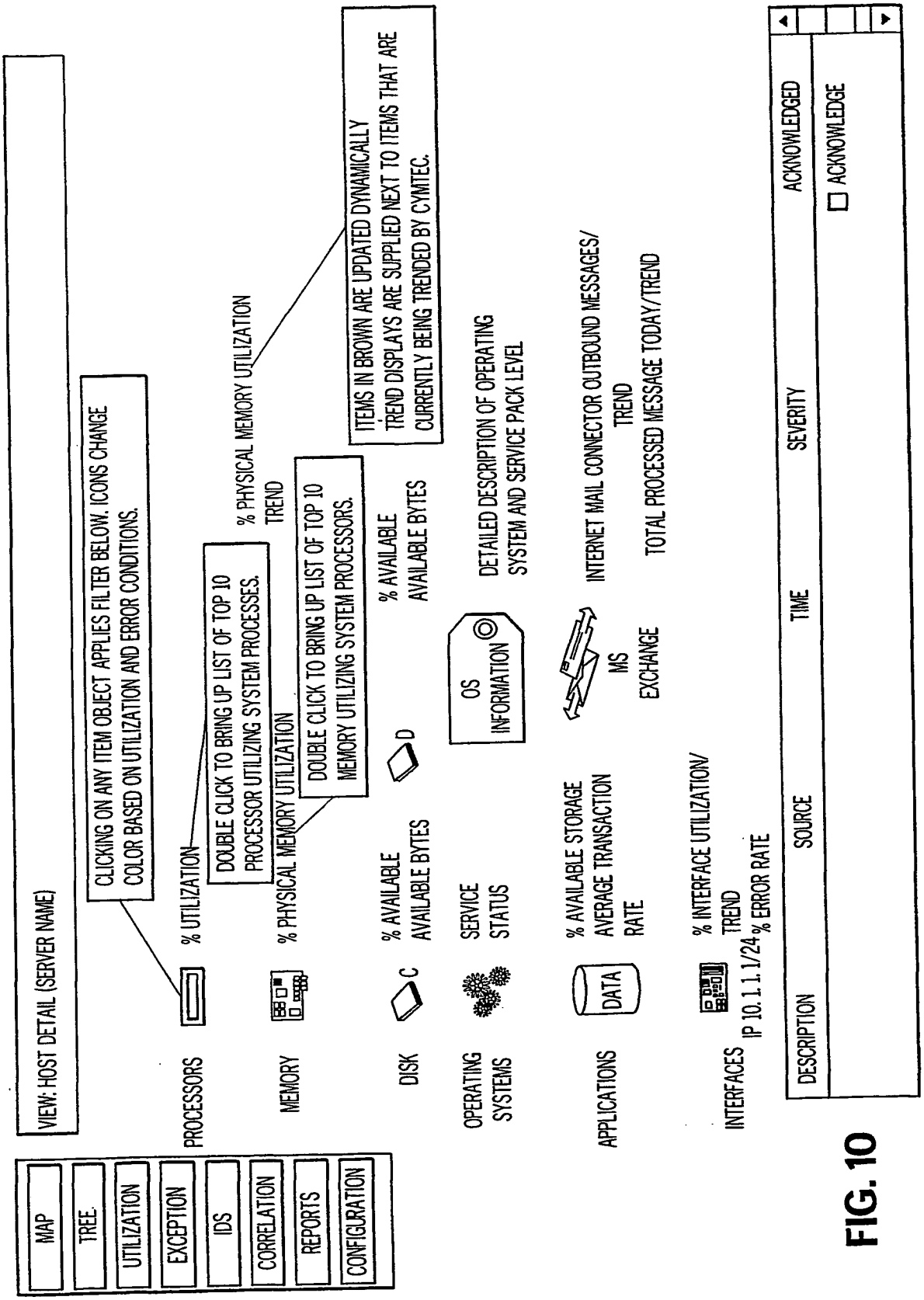


FIG. 10

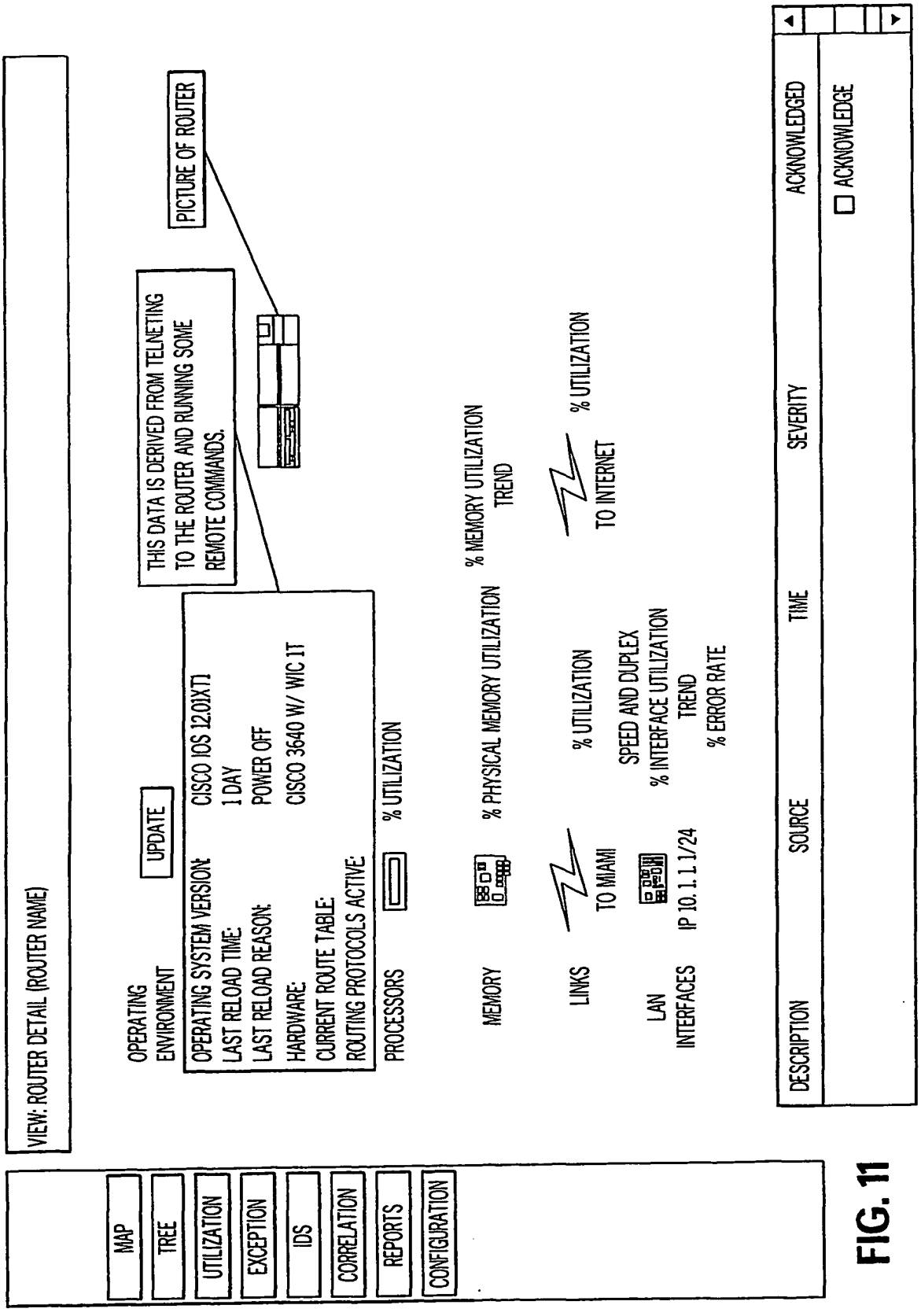


FIG. 11

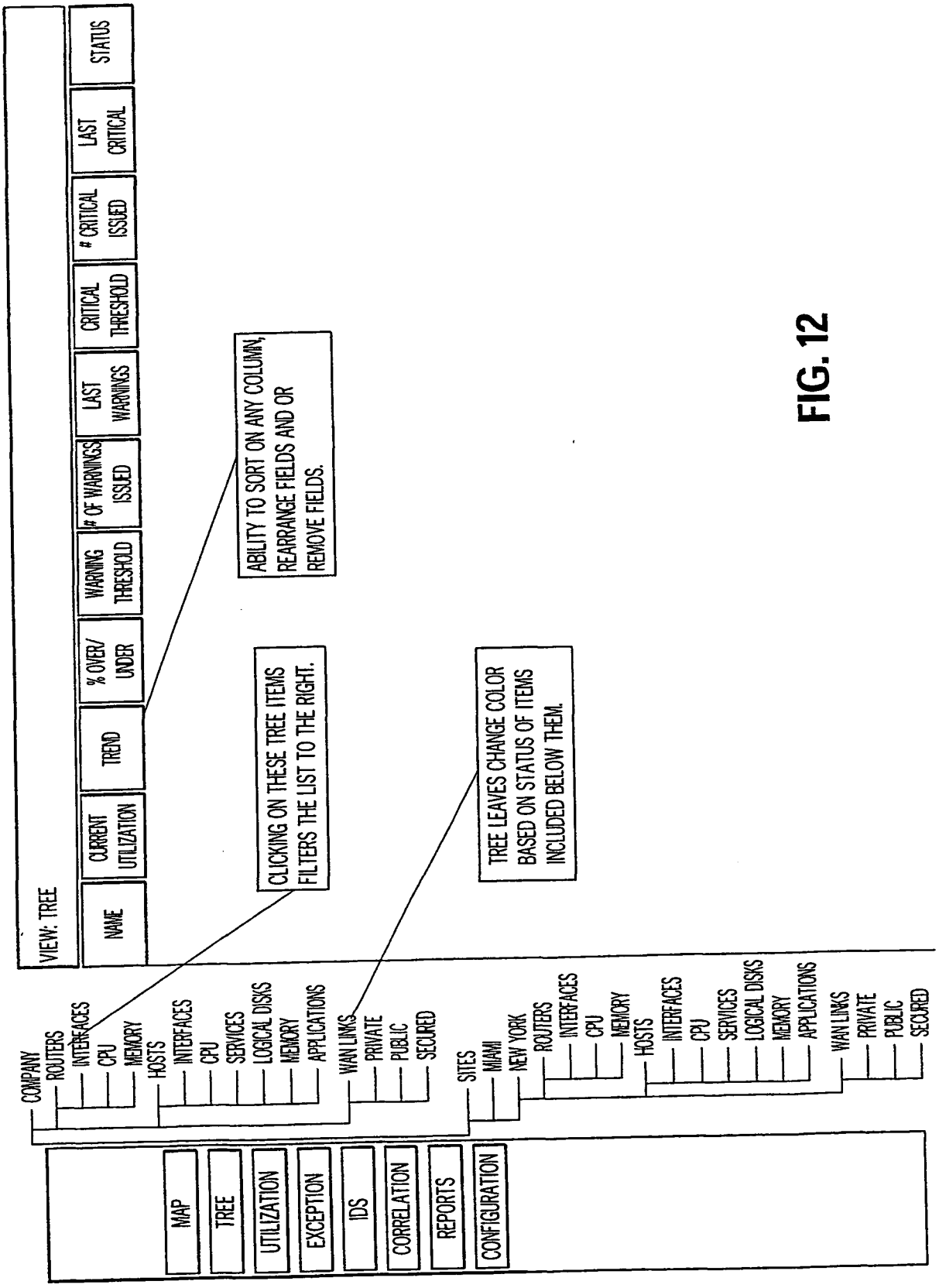


FIG. 12

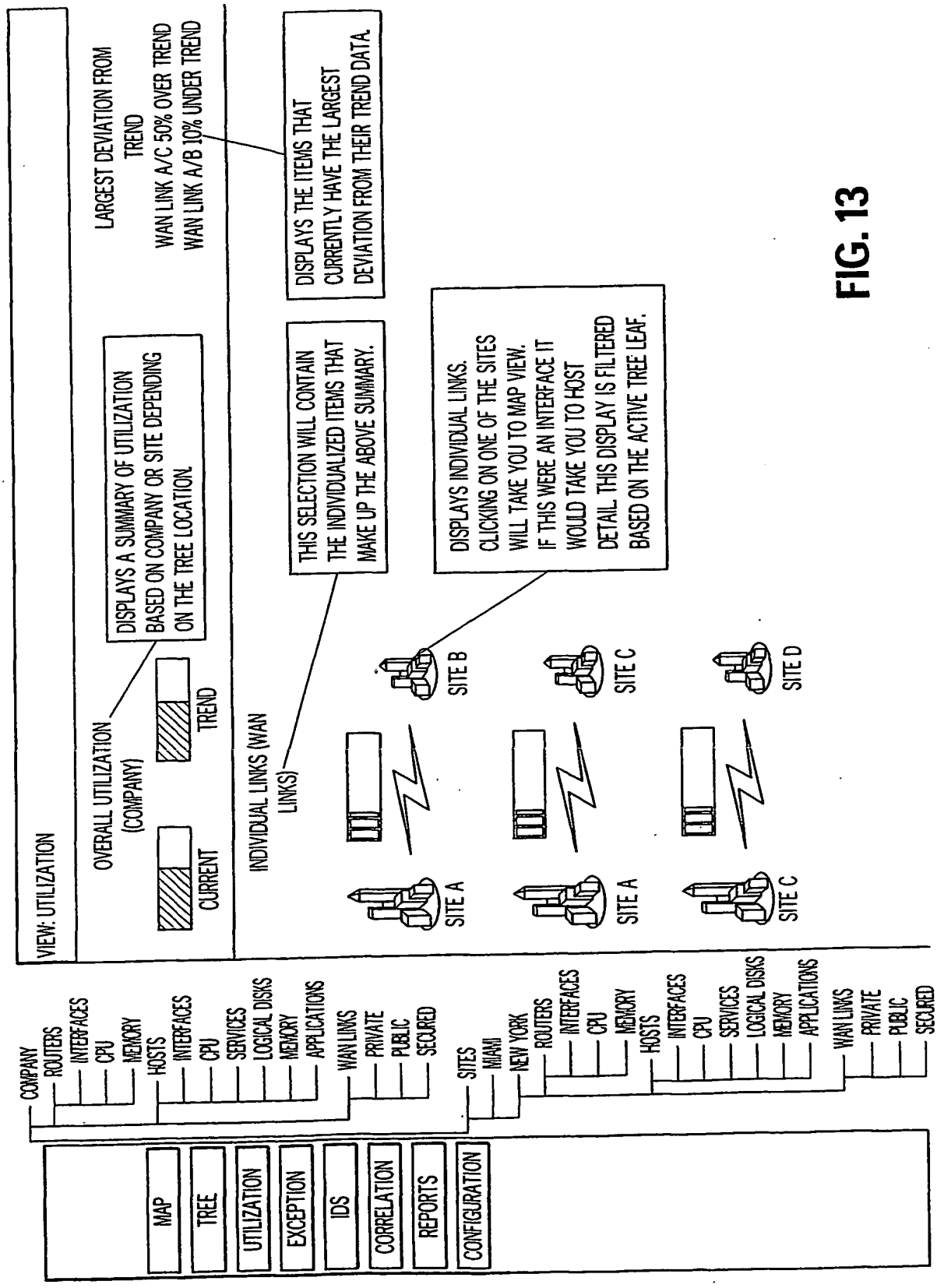


FIG. 13

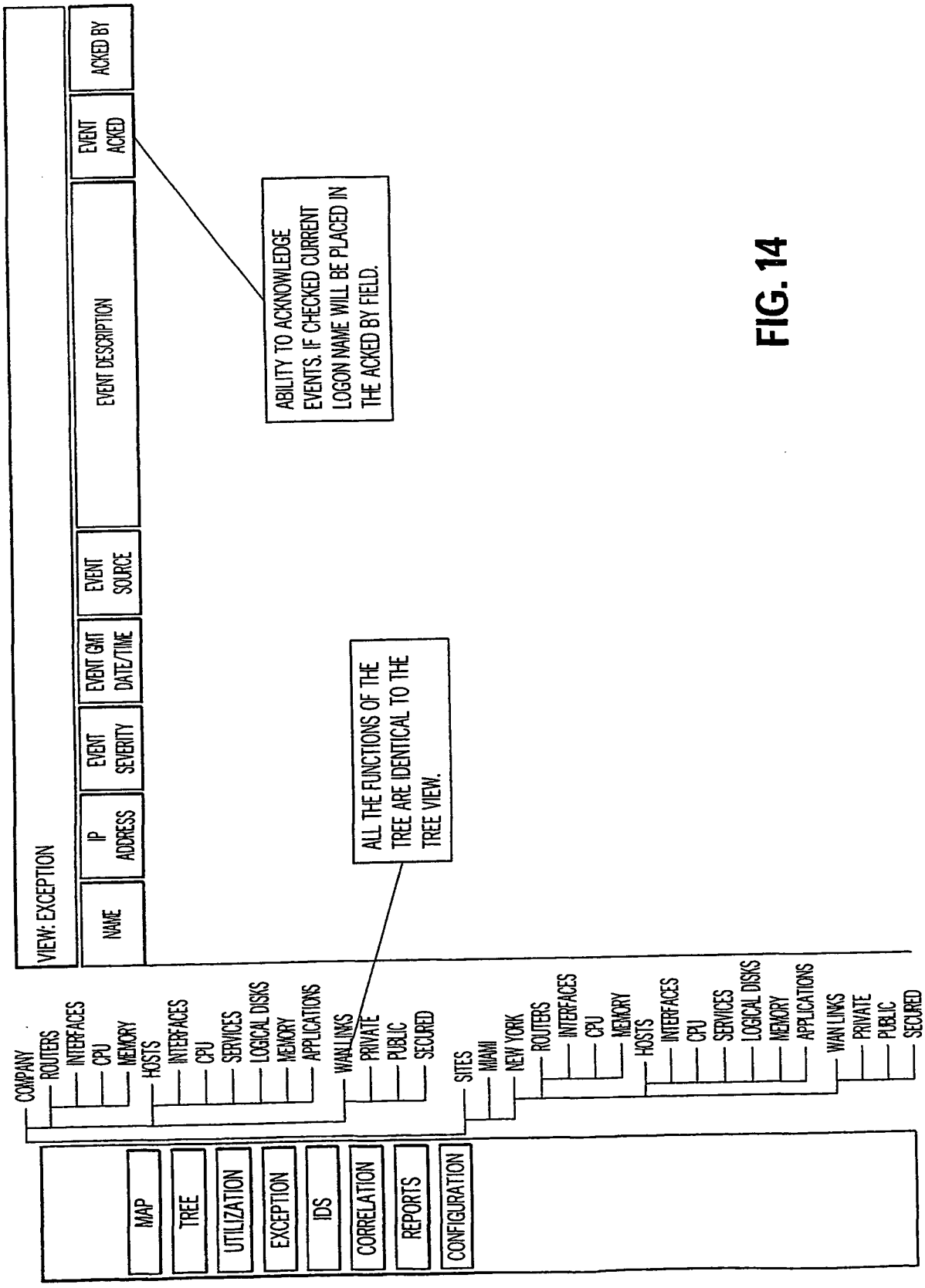


FIG. 14

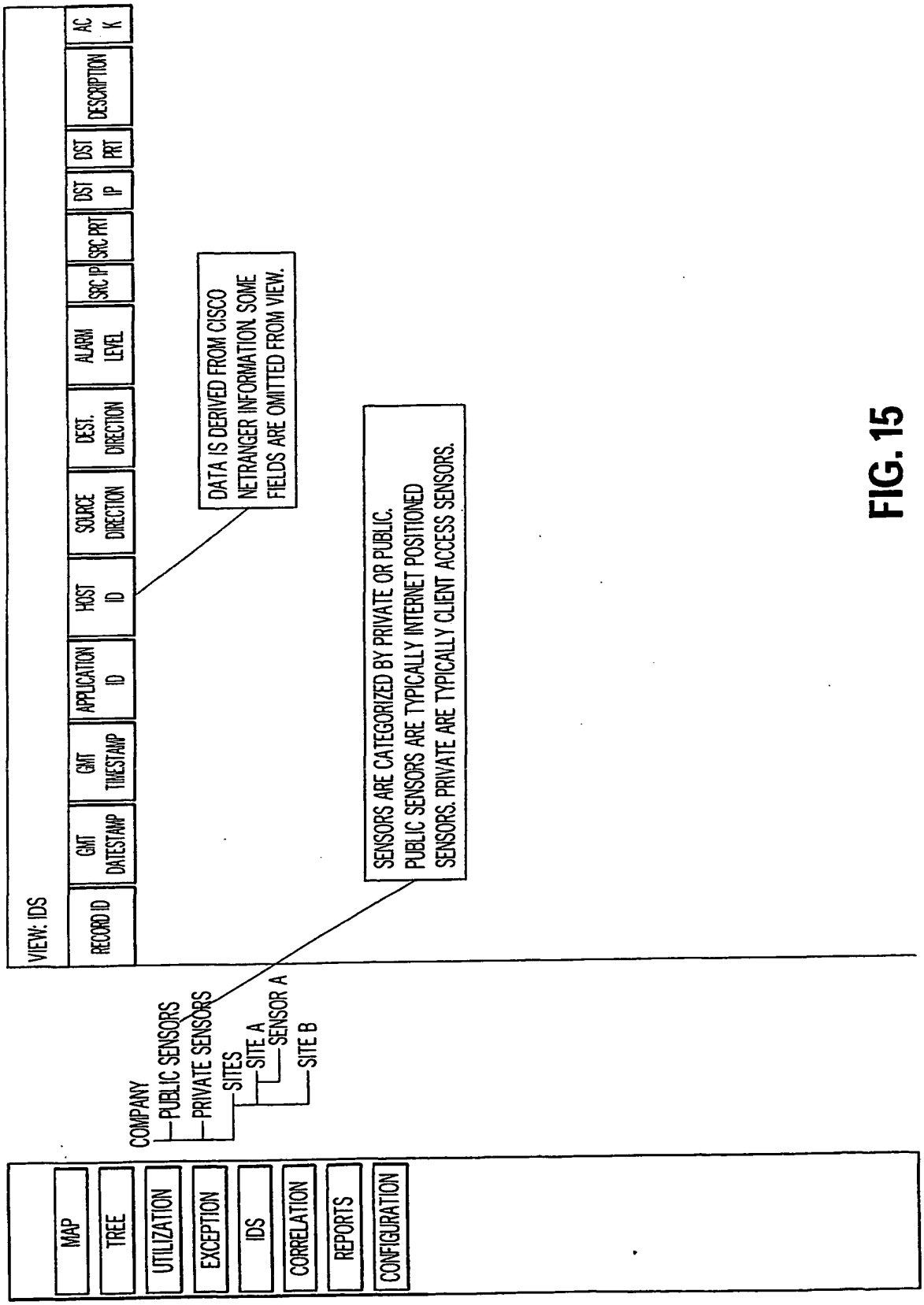


FIG. 15

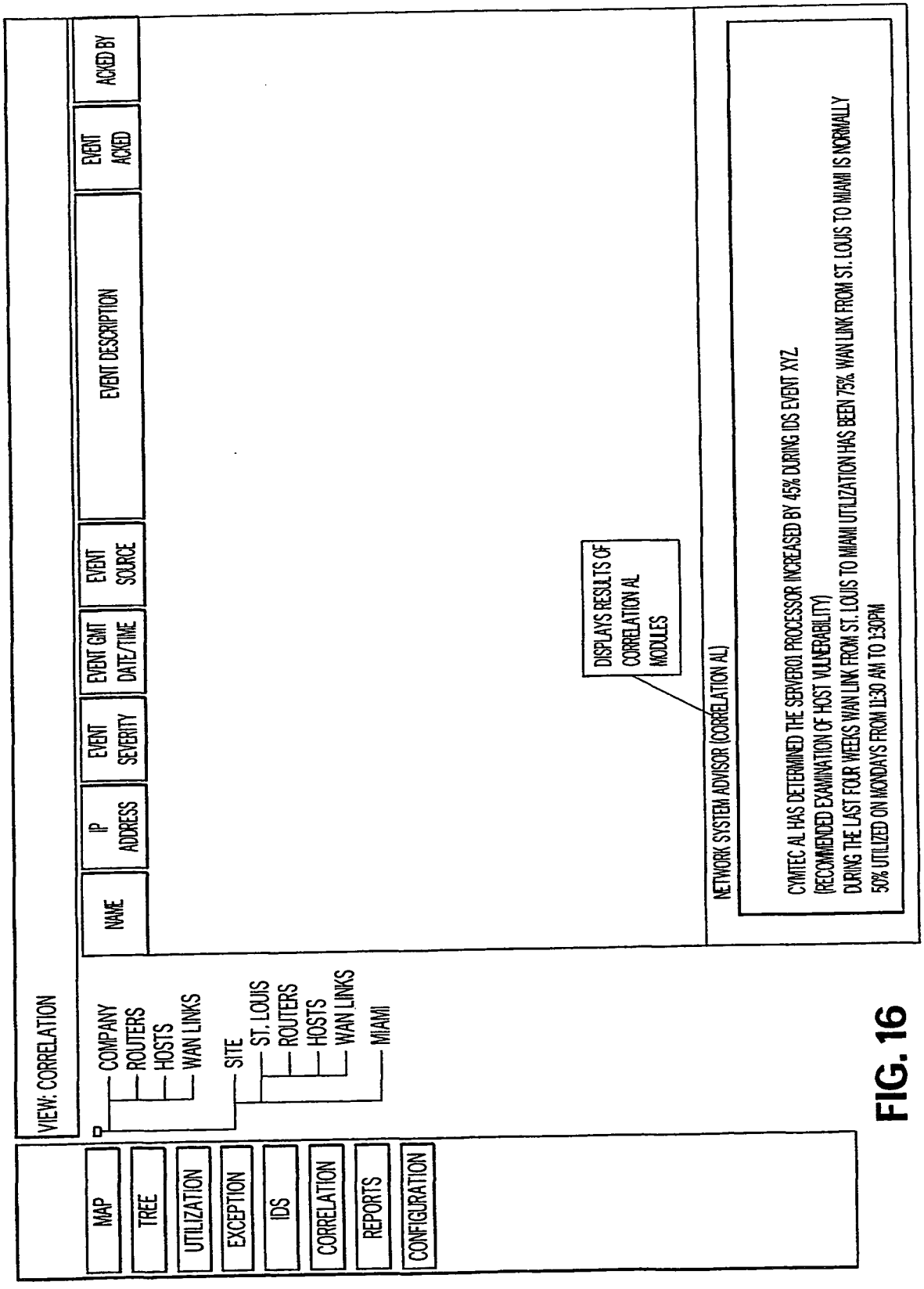


FIG. 16

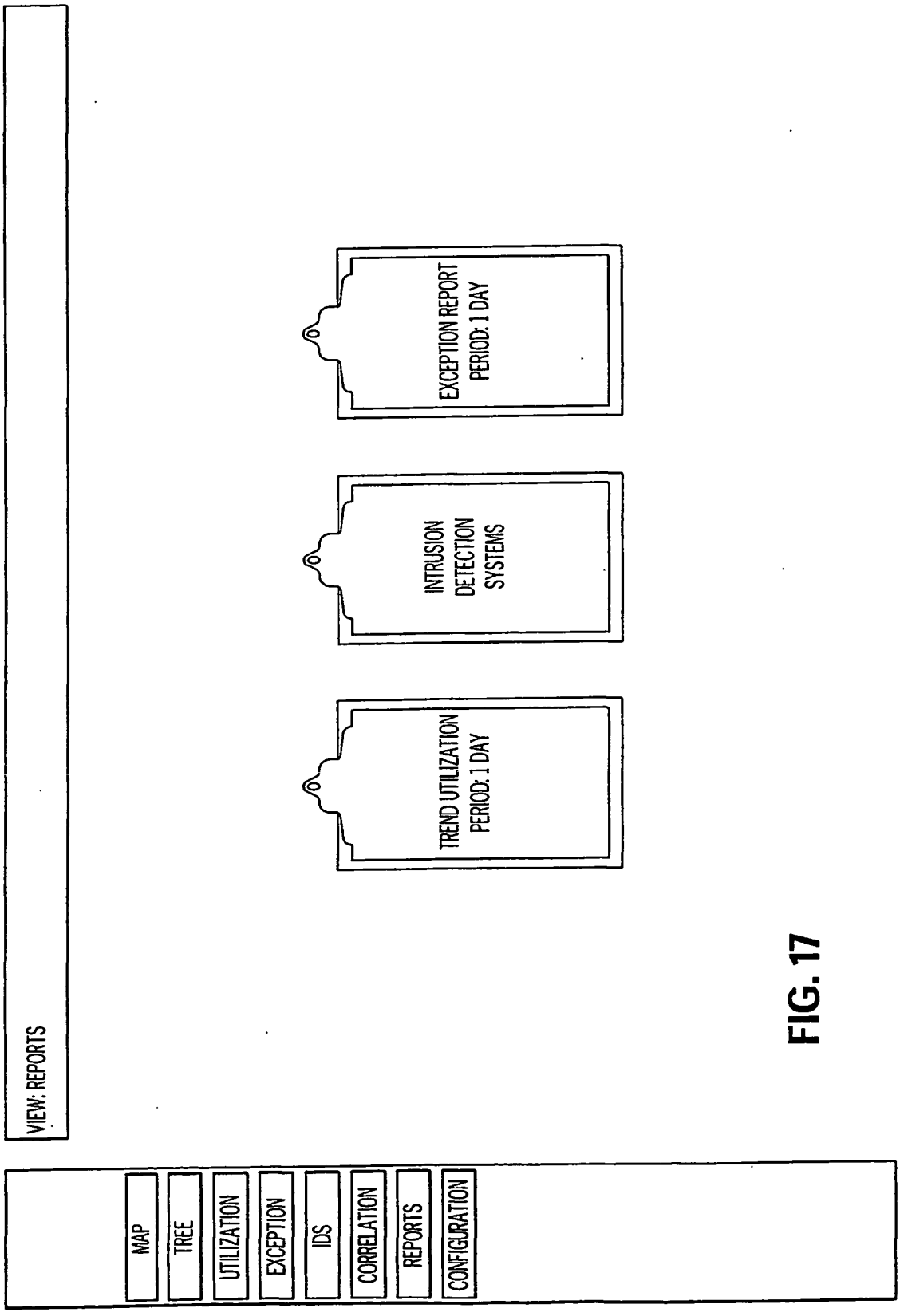


FIG. 17

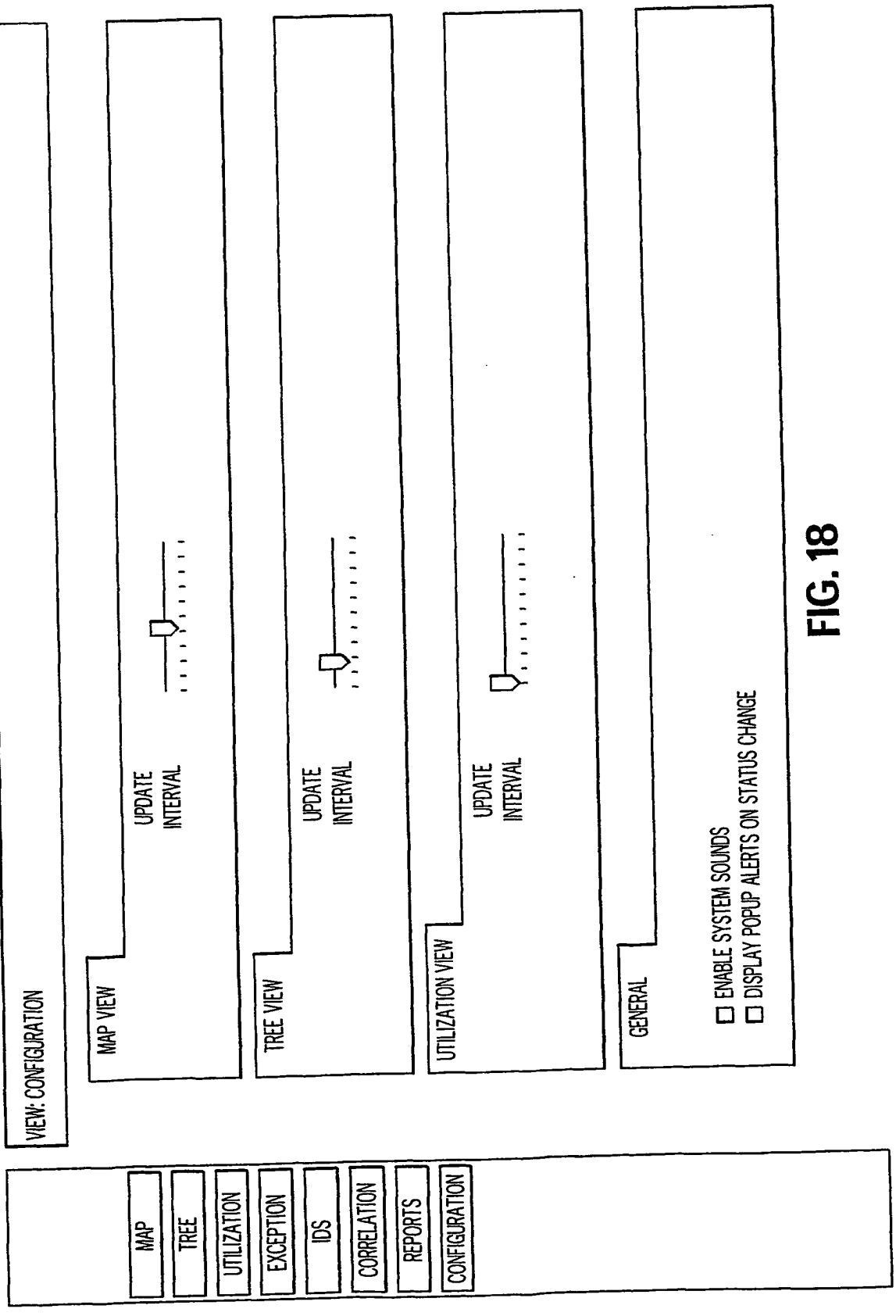


FIG. 18

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number
WO 02/023808 A3

(51) International Patent Classification[7]: H04L 12/24

(21) International Application Number: PCT/US01/28628

(22) International Filing Date:
14 September 2001 (14.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/662,058 15 September 2000 (15.09.2000) US

(71) Applicant: CYMTEC SYSTEMS, INC. [US/US]; 8000 Maryland Avenue, Suite 700, Clayton, MO 63105 (US).

(72) Inventor: MESTER, Michael, L.; 816 C Westbrooke Village Drive, St. Louis, MO 63021 (US).

(74) Agents: KANG, Grant, D. et al.; Thompson Coburn LLP, One Firstar Plaza, St. Louis, MO 60101 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

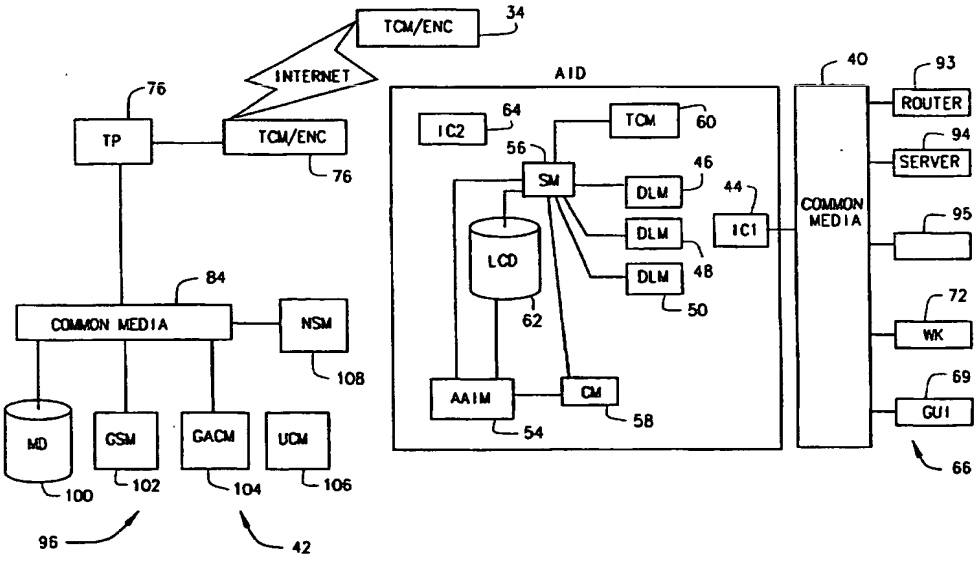
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
16 January 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: NETWORK MANAGEMENT SYSTEM



(57) Abstract: The invention is a network management system that is placed in communication with an existing network. The network management system interposes an intermediate advanced intelligence device between the network management system and the client network. This insertion functions to provide additional security, communication ability and decision-making ability to the management of network systems. The network management system combines trending performance management with intrusion detection to develop an event correlation from multiple data sources. Specifically, data is gathered from multiple sources, a correlation between events and performance data as it relates to security and system optimization, is created, and information is provided to a monitor at the network management system, with additional information provided to a user at the existing network location.

WO 02/023808 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 01/28628

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 951 155 A (BULL SA) 20 October 1999 (1999-10-20) figures 1,2	1-6, 8-12, 15-17
X	page 7, paragraph 47 ---	7
Y	US 5 768 501 A (LEWIS LUNDY) 16 June 1998 (1998-06-16) abstract column 5, line 18 - line 20 --- -/--	1-6, 8-12, 15-17

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 August 2002	28. 10. 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Mannekens, J

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BERNARDI A ET AL: "SPECIFICATION AND ANALYSIS OF A SECURITY MANAGEMENT SYSTEM" PROCEEDINGS OF THE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (NOMS). KISSIMMEE, FEB. 14 - 17, 1994, NEW YORK, IEEE, US, vol. 2 SYMP. 4, 14 February 1994 (1994-02-14), pages 470-485, XP000452342 ISBN: 0-7803-1812-9 page 473, paragraph 1 ---	1-12, 15-17
A	MAILLOT D ET AL: "SECURITY AND INTEGRITY REQUIREMENT ACROSS INTER-DOMAIN MANAGEMENT" GLOBAL INFORMATION INFRASTRUCTURE (GII) EVOLUTION: INTERWORKING ISSUES. INTERWORKING '96. THIRD INTERNATIONAL SYMPOSIUM ON INTERWORKING. NARA (JAPAN), OCT. 1-3, 1996, AMSTERDAM, IOS, NL, 1 October 1996 (1996-10-01), pages 478-492, XP000754594 ISBN: 90-5199-290-4 the whole document ---	1-12, 15-17
A	RABIE S: "Integrated network management: technologies and implementation experience" ONE WORLD THROUGH COMMUNICATIONS. FLORENCE, MAY 4 - 8, 1992, PROCEEDINGS OF THE CONFERENCE ON COMPUTER COMMUNICATIONS (INFOCOM), NEW YORK, IEEE, US, vol. 2 CONF. 11, 4 May 1992 (1992-05-04), pages 1020-1027, XP010062180 ISBN: 0-7803-0602-3 the whole document ---	1-12, 15-17
A	MANSFIELD G ET AL: "The MIKB model for intelligent network management" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON COMMUNICATIONS (ICC). GENEVA, MAY 23 - 26, 1993, NEW YORK, IEEE, US, vol. 3, 23 May 1993 (1993-05-23), pages 1210-1214, XP010137050 ISBN: 0-7803-0950-2 the whole document ----	1-12, 15-17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 01/28628

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this International application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-12,15-17

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-12,15-17

   "A method of managing a network"

2. Claims: 13-14

   "A method of extracting data from a network"

3. Claims: 18-19

   "A method of configuring an agent"

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 01/28628

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0951155	A	20-10-1999	FR	2777723 A1	22-10-1999
			EP	0951155 A1	20-10-1999
			US	6430613 B1	06-08-2002
US 5768501	A	16-06-1998	US	6000045 A	07-12-1999
			US	6205563 B1	20-03-2001
			US	2001013107 A1	09-08-2001